United States
Nuclear Regulatory Commission

NRC Electronic Information Exchange (EIE) Instructional Guide

Electronic Document Submittal Procedure

Chief of the Information Officer
Information Management Division

November 17, 2000

TABLE OF CONTENTS

1.0 INTRODUCTION

1.1 Background

The Agencywide Documents Access and Management System (ADAMS) has been developed to be the NRC's electronic document and records management system. An integral part of ADAMS is the capability to process and disseminate electronic documents that are either received into the Agency or are created within the Agency. The process providing this capability is called Electronic Information Exchange (EIE). EIE allows both users internal to NRC as well as those external to NRC to exchange electronic documents in a secure and valid manner via the Internet.

The development and use of EIE in the NRC environment are intended to address the mandate of the Government Paperwork Elimination Act, Title XVII of Public Law 105-277, that provides for Federal agencies, by October 21, 2003, to give persons who are required to maintain, submit, or disclose information the option of doing so electronically. It is also intended to provide for the use of electronic authentication (electronic signature) methods to verify the identity of the sender and the integrity of electronic content where necessary. The Act specifically provides that electronic records and their related electronic signatures are not to be denied legal effect, validity, or enforceability merely because they are in electronic form.

The NRC is in the implementation stage of the NRC EIE program. The objective of the program is to institute business processes that enable the NRC and the customers and clients of the NRC to interact and communicate electronically in a secure manner via the Internet. In addition, the objective is to document and preserve electronic submissions and transmissions in a manner consistent with that for paper documents. Finally, this undertaking is expected to provide the basis for further evaluation and analysis enabling operational and procedural improvements to the EIE process prior to Agency-wide implementation.

1.2 EIE Business Description

The NRC EIE system design is based on a public key infrastructure (PKI) that provides the capability to exchange electronic documents in a secure manner via the Internet using Secure Sockets Layer (SSL3) technology. In addition, it incorporates the use of digital signature technology to provide submitter (sender) validation and document authentication. The purpose of this document is to provide instructions for participation in the EIE Program.

1.3 Who Can Participate

The participant population includes the NRC and its customers and clients who choose to electronically submit regulatory required submittals in compliance with 10 CFR Part 50.4. The participants internal to the NRC will include offices whose customers and clients choose the EIE process to submit documents electronically in a secure and valid manner via the Internet. The offices will designate individual users who have the responsibility for originating, signing, or receiving official submittals into the Agency. Participants external to the NRC will include those individuals designated having the responsibility of originating, signing, or sending documents to the NRC in compliance with 10 CFR Part 50.4.

1.4 How to Register

The NRC provides for overall administration of the EIE process through the designated Local Registration Authority (LRA). The LRA creates and maintains an Authorized Certificate List (ACL) consisting of authorized internal and external EIE participants. Each participant must send an ACL containing the name and e-mail addresses of individuals who will be submitting digitally signed documents to the NRC. The ACL must be sent to the NRC in a signed paper form to the following address:

U.S. Nuclear Regulatory Commission
Electronic Information Exchange
License Registration Authority T6 C30
Washington, D.C. 20555

Upon receipt of the ACL, the NRC will e-mail to each individual named a unique personal identification number (PIN) to be used in applying for a digital certificate. Once received, the digital certificate will then enable the individual users to digitally sign documents and submit them in a secure manner. The PIN number will be sent approximately 3 to 5 days after receipt of the ACL. Addressees may add or delete names from the ACL by written notification to the NRC using the above address.

The LRA will use the ACL to validate authorized individuals requesting digital signature certificates. The LRA may be contacted via e-mail at pgn1@nrc.gov.

1.5 What is Needed to Participate

Participating individuals in the EIE initiative may use their existing workstations with standard desktop configuration. The recommended workstation configuration requires a Pentium 133 Mhz (or higher) with a minimum of 32 MB of RAM, 20 MB of available disk space, and access to the World Wide Web (web) through an Internet Service Provider (ISP). The operating system should be either Windows NT or Windows 95 (or higher). In addition, each workstation must be equipped with browser software consisting of either Netscape Navigator or Communicator (version 4.6 or higher) or Microsoft Internet Explorer (version 5.0). Other browser types such as AOL or Mosaic are not currently

supported for use in the EIE process. All other software needed in the EIE process will be available via the NRC EIE external server home page or designated URLs. Listed below are the specific software plug-ins required, their file names, and the URLs where they can be obtained.

Software/Plug-ins	File Name	Location (Download from)
InternetForm Viewer (Browser Application)	IFV431G.EXE	www.nrc.gov/NRC/EIE/index.html EIE Start Up (Step 1)
Netscape 4.x plug-in (signaturing piece)	IFXNDSS.EXE	www.nrc.gov/NRC/EIE/index.html EIE Start Up (Step 2)
Microsoft Internet Explorer 4.x plug-in (viewer patch)	MASQ_URL.EXE	www.nrc.gov/NRC/EIE/index.html EIE Start Up (Step 2)
Digital ID Certificate		www.nrc.gov/NRC/EIE/index.html Request/Retrieve Certificate (Step 3)

Table 1-1: Required Software

2.0 HOW TO START USING EIE SYSTEM

2.1 Introduction

In order to utilize EIE, each individual must obtain a digital signature certificate (Digital ID). Additionally, each of the software plug-ins listed above in Table 1-1 must be downloaded and installed. In the succeeding sections, each process and step required to set-up a computer or workstation to use EIE is described. The processes and steps described are specific to both Netscape Navigator/Communicator 4.6 or higher and Microsoft Internet Explorer 5.0.

2.2 How to Obtain a Digital ID Certificate

All users must have a Digital ID in order to use EIE. (Refer to the Glossary of Terms for a full description of a Digital ID certificate.) A Digital ID is used to submit and digitally sign the form used to submit documents and is required in order to access the EIE external server and retrieve documents. The EIE system requires the use of an NRC issued Digital ID.

To obtain a Digital ID, authorized participants (applicants) must first complete and submit an enrollment form. VeriSign, Inc. acts as the NRC's Certificate Authority (CA) and provides the NRC with a Digital ID enrollment page on their web site. The NRC provides VeriSign Onsite Digital ID's at no cost. The steps for obtaining a Digital ID are as follows:

Step 1: Applicants can apply for a Digital ID by accessing the EIE home page at www.nrc.gov/NRC/EIE/index.html . When the NRC EIE home page appears, click on the Request/Retrieve Certificate hyperlink.

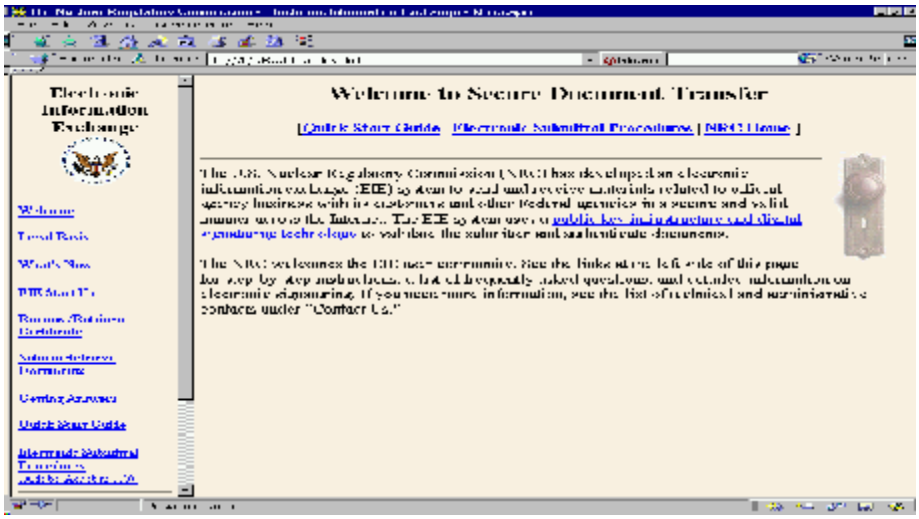

Figure 2-1: EIE Home Page

Step 2: From the Request/Retrieve Certificate page, go to Step 3. **Click on Go to the VeriSign/NRC Page**.

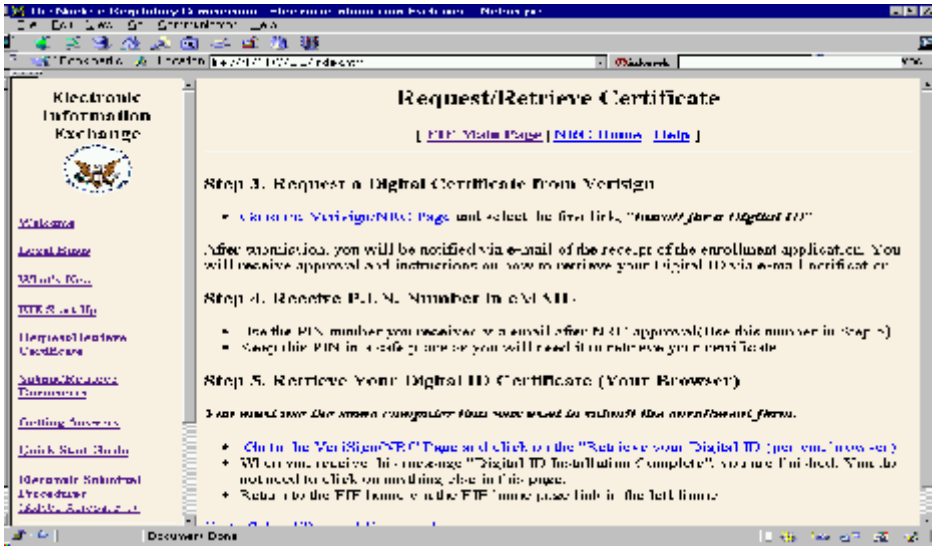

Figure 2-2: Request/Retrieve Certificate Page

Step 3: Once connected, the VeriSign Onsite End-User User Services page appears at (https://onsite.verisign.com/USNuclearRegulatoryCommissionADDOCIO/index.html). Applicants begin the enrollment process by selecting the first option presented, "Enroll for a Digital ID."

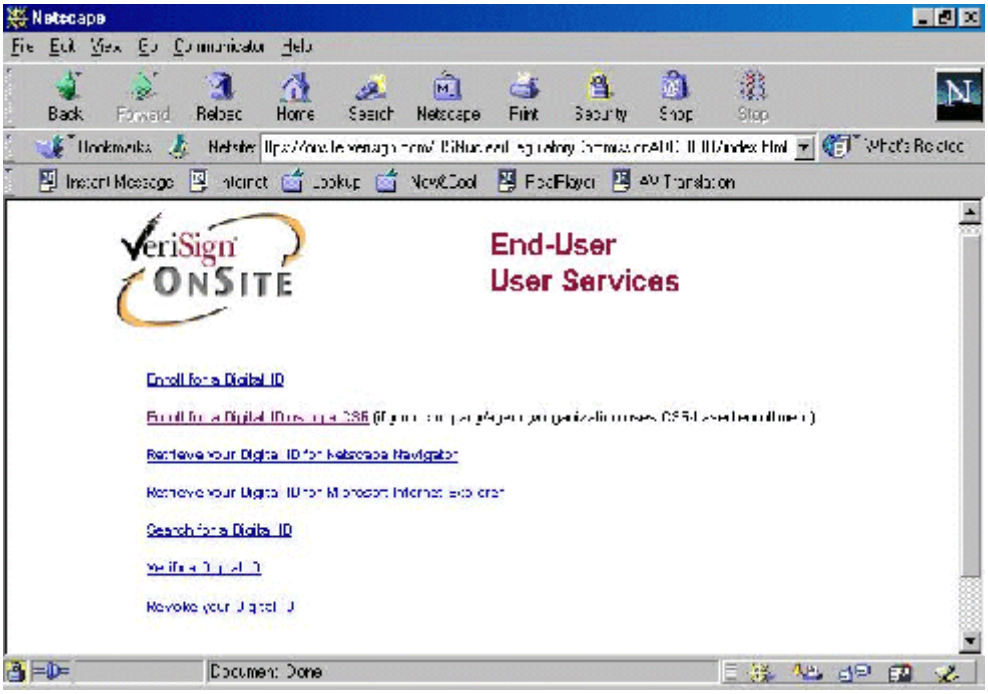

Figure 2-3: NRC VeriSign Onsite Enrollment Page

After selecting this option, the applicant is presented with an online enrollment form. When enrolling, applicants must use the same computer on which they intend to install the Digital ID and private key.

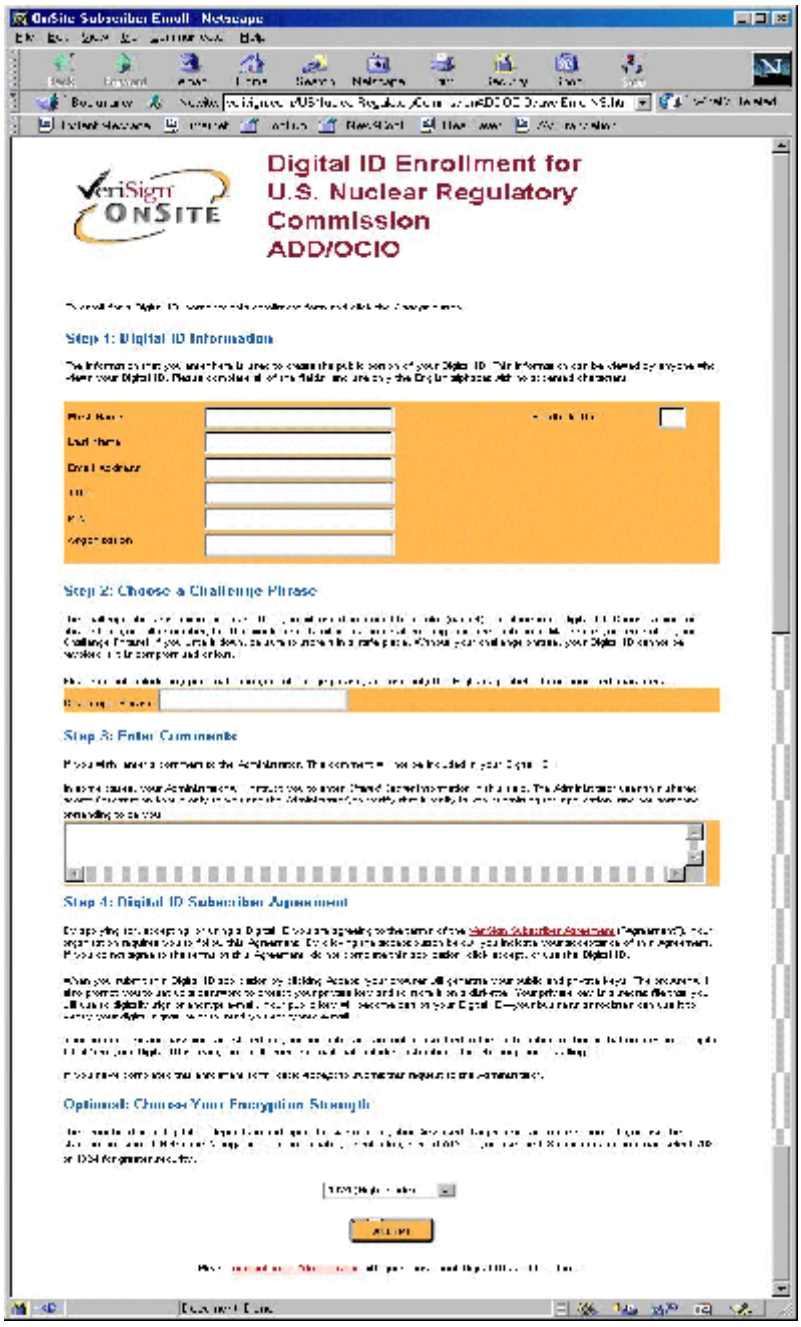

Figure 2-4: Digital ID Enrollment Form

Step 4: The form is divided into five parts. Applicants must complete all required information on the enrollment form as follows:

1. **Digital ID Information** - Applicants must complete the first name, middle initial, last name, e-mail address, title, PIN, and organization fields. Applicants will be prompted to enter the e-mail address twice to confirm it. The title should reflect the applicant's position in the organization. The PIN number to be entered is supplied by the NRC subject to the submission of the Authorized Certificate List. The organization should state the corporate entity or plant name where the applicant is employed.

2. **Choose a Challenge Phrase** - Applicants must enter a word or phrase that serves to validate their identity should a situation arise that requires the Digital ID to be canceled or revoked. (Note: Your Digital ID can not be renewed without your Challenge Phrase. Because renewal only occurs once a year, be sure to write down the Challenge Phrase and keep it in a safe place.)

3. **Enter Comments** - This part is optional.

4. **Digital ID Subscriber Agreement** - Each applicant is encouraged to read and understand the subscriber agreement.

5. **Choose your Encryption Strength** - Encryption strength refers to the security of the Digital ID. The longer the encryption key the more secure the Digital ID. It is recommended that applicants select the largest key size that can be handled by your browser. (Older browser versions will default to 512 bit keys whereas newer browser versions can handle up to 1024 bit keys.)

Step 5: Submit the enrollment form by clicking on the **Accept** button. You will receive a prompt to make certain your e-mail address is correct. Follow the instructions on the dialog box and click on the **OK** button.

Figure 2-5: E-mail Address Confirmation

Step 6: Upon submission of the enrollment form, the applicant is prompted to initiate the generation of the private key as illustrated below. Click on the **OK** button.

Figure 2-6: Generate a Private Key

After clicking on the **OK** button, users of Netscape browsers will be prompted to enter a password for the Certificate Database.

Figure 2-7: Netscape Password Entry Dialog

Step 7: Enter a unique password and click on the **OK** button. You will be prompted to re-enter it for confirmation. (Note: Be sure to choose a password that is easy to remember, yet secure. This is a must since the access to and use of your Digital ID will depend on this password. If you must, write the password down and keep it in a safe place.)

Once the Certificate Database password is entered and confirmed, the Netscape user is returned to the Generate a Private Key dialog.

Figure 2-8: Generate a Private Key

Step 8: Click on the **OK** button to generate a key. A private key is automatically generated and stored in the browser.

This completes the enrollment process. A window appears stating the enrollment is complete and that the LRA will review their enrollment application and notify them of the results by e-mail.

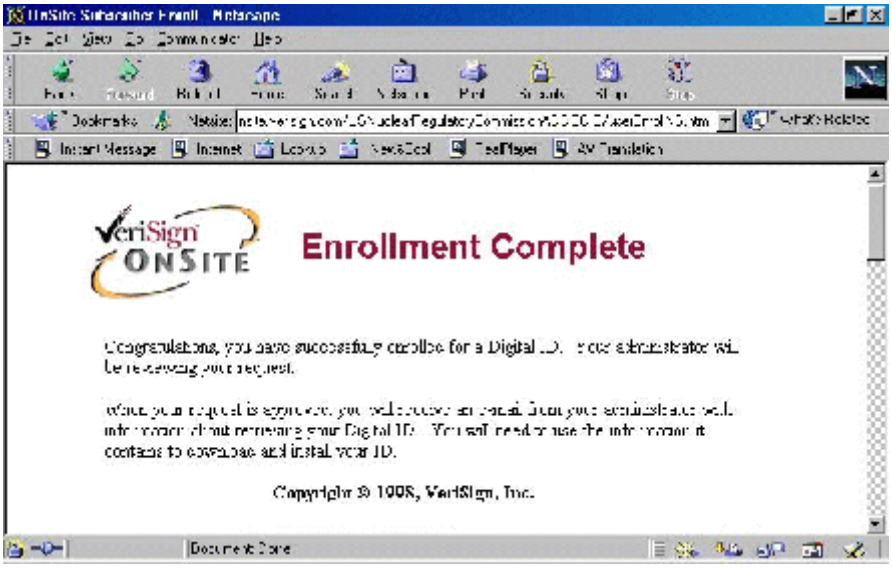

Figure 2-9: Enrollment Complete

2.3 Establishing Private Key Security

Both Netscape Navigator/Communicator and Microsoft Internet Explorer users can establish password security to protect their private key. The steps applicable to each are outlined below.

Netscape Navigator/Communicator (version 4.6 or higher)

In the case of Netscape, the private key is stored in the Certificate Database which is password protected. The Certificate Database is established during the generation of the private key. (See Section 2.2). You may, however, change your password. This is accomplished as follows.

Step 1: Click on the **Security** icon on the Netscape toolbar.

Figure 2-10: Netscape Toolbar

The Security Info window appears.

Figure 2-11: Security Info Window

Step 2: Click on **Passwords**. This invokes the Netscape Passwords window.

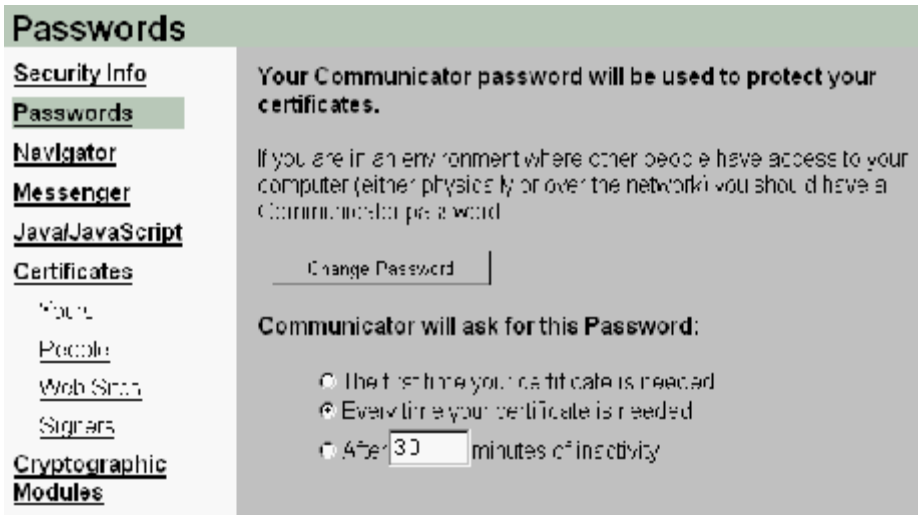

Figure 2-12: Netscape Passwords Window

Step 3: Click on the **Change Password** button. This produces the Certificate Database (DB) password entry dialog.

Figure 2-13: Netscape Certificate Database Password Entry

Step 4: Enter your old password. Then enter a unique password and re-enter it to confirm it. Then click on the **OK** button. This establishes a password protected Certificate Database. (Note: Be sure to choose a password that is easy to remember, yet secure. This is a must since the access to and use of your Digital ID will depend on this password. If you must, write the password down and keep it in a safe place.)

Microsoft Internet Explorer (version 5.0 or higher)

Microsoft Internet Explorer users will be allowed to assign additional security to their private key when enrolling for a Digital ID.

Step 1: After clicking to generate a private key, the Additional Security dialog box appears.

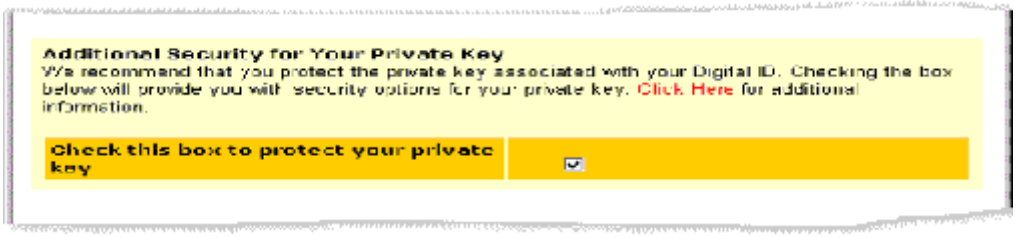

Figure 2-14: Microsoft Additional Security Dialog

Step 2: If you do not check the box, a private key will be generated. However, if you desire additional security for your private key, place the cursor in the box and click to check the box. In so doing, you will be prompted to choose an appropriate security level. The three security levels - high, medium, or low - are described below.

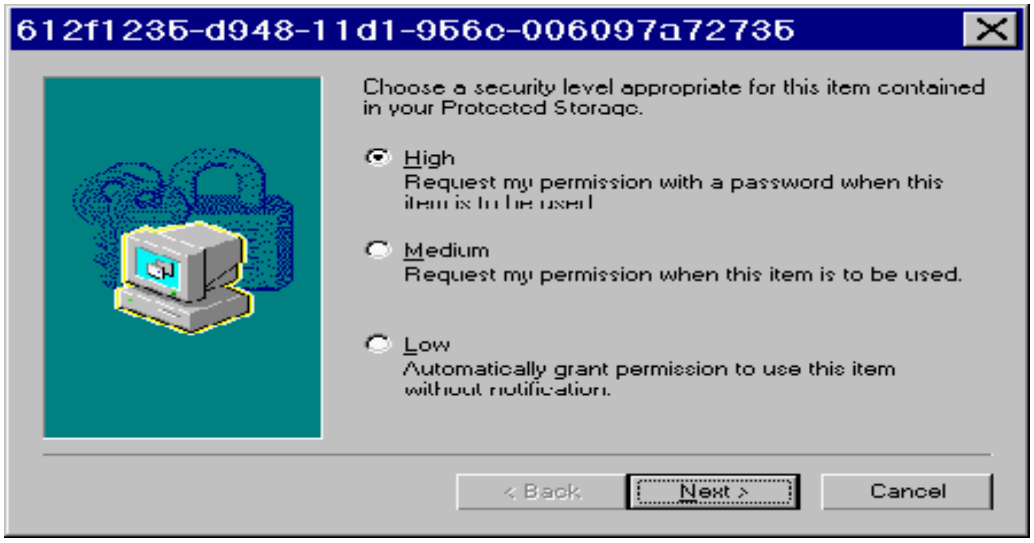

Figure 2-15: Microsoft Security Level Window

High - Requires you to enter a password before your private key is accessed.

Medium - Alerts you and asks for permission before your private key is accessed.

Low - Does not add any additional security. Your private key is protected only by your system's logon procedure.

If you select the “high” security option, you will be prompted to assign a password.

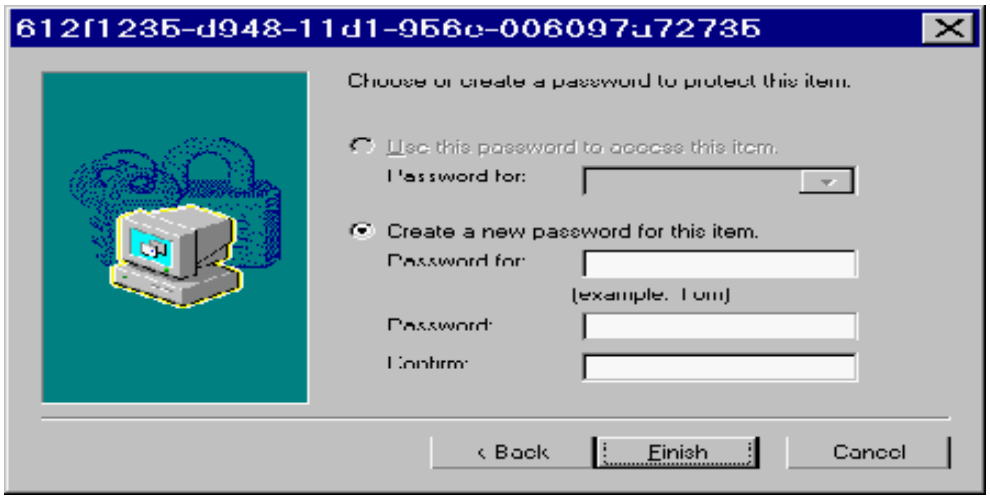

Figure 2-16: Microsoft Password Entry

Step 3: After entering and confirming the password, click the **Finish** button. A final window appears asking for the password and allowing the generation of the private key by clicking on the **OK** button.

Figure 2-17: Microsoft High Security

2.4 Approving the Digital ID Certificate

The Digital ID enrollment form is transmitted to the LRA via a secure link using SSL3. When the form is submitted to the LRA, an e-mail message is generated and sent to the applicant acknowledging it’s receipt. (See Appendix A.) The LRA validates the information contained in the form using the ACL. If the information matches that in the ACL, the LRA approves the issuance of a Digital ID certificate. If the information does not

match that in the ACL, the LRA shall deny the issuance of a Digital ID certificate. In either case, an e-mail message is generated to the applicant notifying them of the decision.

Each applicant is expected to be approved unless he or she did not receive authorization or failed to properly register with the LRA. In the case of a disapproved request, the LRA will provide e-mail notification of the disapproval and will endeavor to provide a specific reason for it. (See Appendix B.) Once the applicant appropriately addresses the reason for disapproval, a new enrollment form can be submitted. The LRA shall serve as the point of contact for any questions related to the enrollment process and shall make every effort to process requests for Digital IDs within two business days of receipt.

2.5 Retrieving and Installing the Digital ID Certificate

Upon approval, applicants are notified of the decision via e-mail. The e-mail shall contain instructions on how to access and retrieve the Digital ID certificate. (See Appendix C.) The e-mail instructions shall include the following:

1. Statement of the URL where the digital certificate can be retrieved.

2. The personal identification number (PIN) needed to retrieve the digital certificate, e.g., 892137890.

3. Statement to follow instructions on the web page to complete installation of the digital certificate (Digital ID).

To retrieve and install the Digital ID, applicants must use the same computer used to submit the enrollment form. To successfully install the Digital ID, follow the steps listed below.

Step 1: With the e-mail open, copy the PIN by highlighting it and pressing the “Ctrl” and “C” keys at the same time or by highlighting it, right clicking with your mouse, and selecting copy from the shortcut menu.

Step 2: Click on the URL provided in the same e-mail message, i.e., (https://onsite.verisign.com/USNuclearRegulatoryCommissionADDOCIO/index.html.)

Step 3: Once connected, the participant is presented with the VeriSign OnSite Host page for NRC.

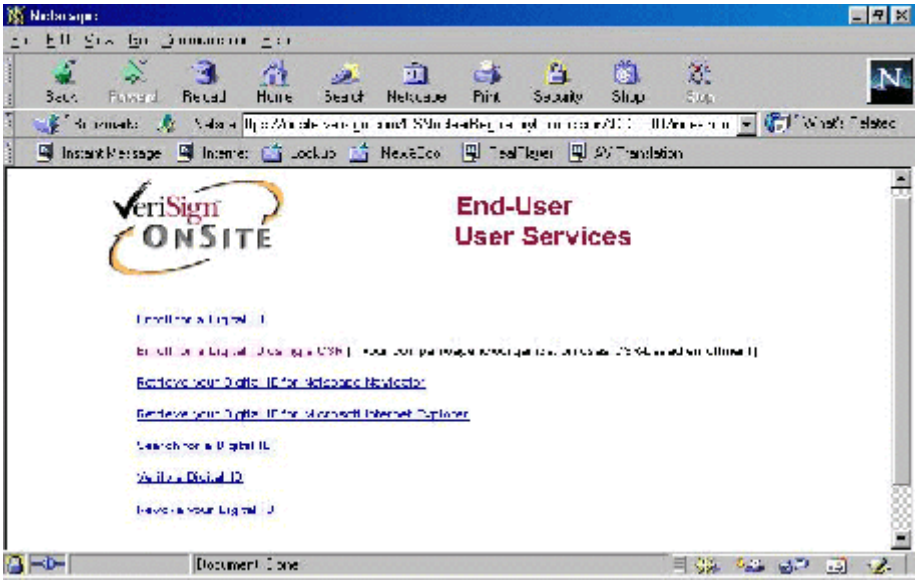

Figure 2-18: NRC VeriSign OnSite Host Page

Of the options presented, options 3 and 4 are for retrieval of a Digital ID. Depending on whether your browser is Netscape Navigator/Communicator or Microsoft Internet Explorer, select the appropriate option.

The participant is presented with the VeriSign Digital ID Services window that allows the participant to "Pick up your Digital ID."

Step 4: Paste the **PIN** number provided in the e-mail (and copied in Step 1) in the Digital ID PIN box by clicking your cursor within the box and pressing the "Ctrl" and "V" keys at the same time or right clicking and selecting **Paste** from the shortcut menu.

Figure 2-19: Pick Up Your Digital ID

Step 5: Click on **Submit** to install your Digital ID. (Note: Netscape users are prompted to enter their certificates database password before installation proceeds.) When the installation is complete, a Congratulations message will appear indicating a successful

download and installation. In addition, it will contain instructions on how to check to ensure proper installation.

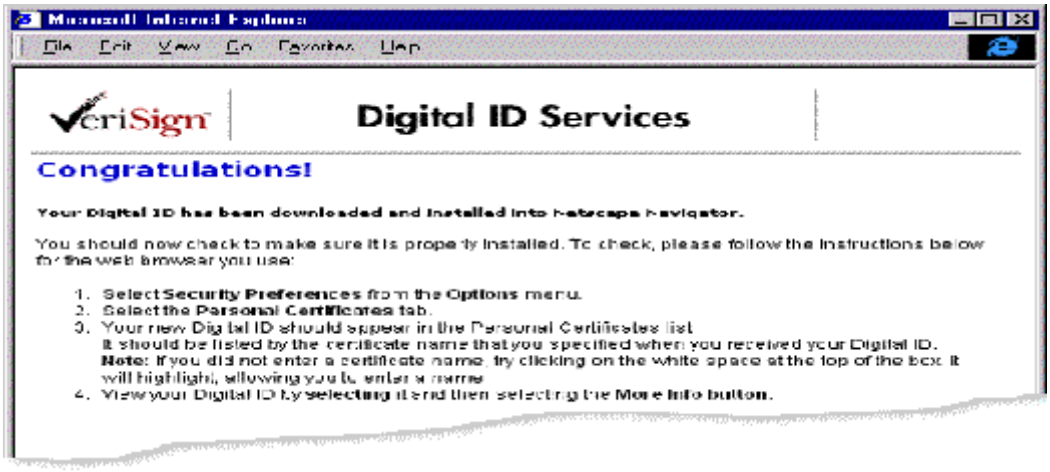

Figure 2-20: Successful Download and Installation

2.6 Verifying Successful Installation

Once the installation process is complete, the participant is encouraged to check or verify the installation of their Digital ID certificate. The process of verifying installation is similar for both Netscape Navigator/Communicator and Microsoft Internet Explorer users. The steps applicable to each are outlined below.

Netscape Navigator/Communicator (version 4.6 or higher)

Step 1: Click on the **Security** icon on the Netscape toolbar.

Figure 2-21: Netscape Toolbar Security Icon

Step 2: The Security Advisor/Info window opens. Select **Yours** from the left hand margin under Certificates. Your Digital ID should appear in the "These are your certificates" window. Highlight your Digital ID and click on the **View** button.

Figure 2-22: Your Certificates Window

Step 3: Your Digital ID should appear in the "These are your certificates" window. Highlight your Digital ID and click on the **View** button to display the contents of your Digital ID.

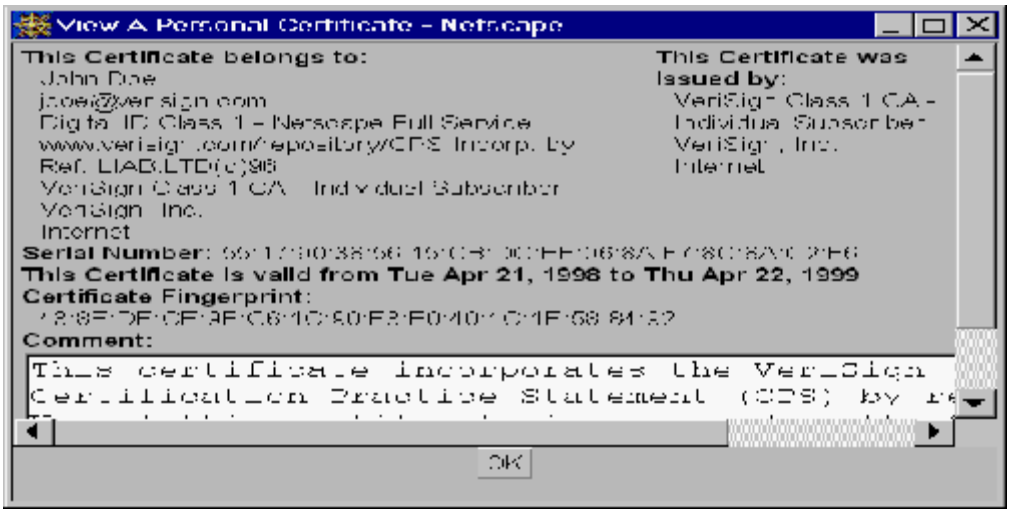

Figure 2-23: Personal Certificate

Microsoft Internet Explorer (version 5.0 or higher)

Step 1: Select **View** from the menu bar and click on **Internet Options** on the drop down menu.

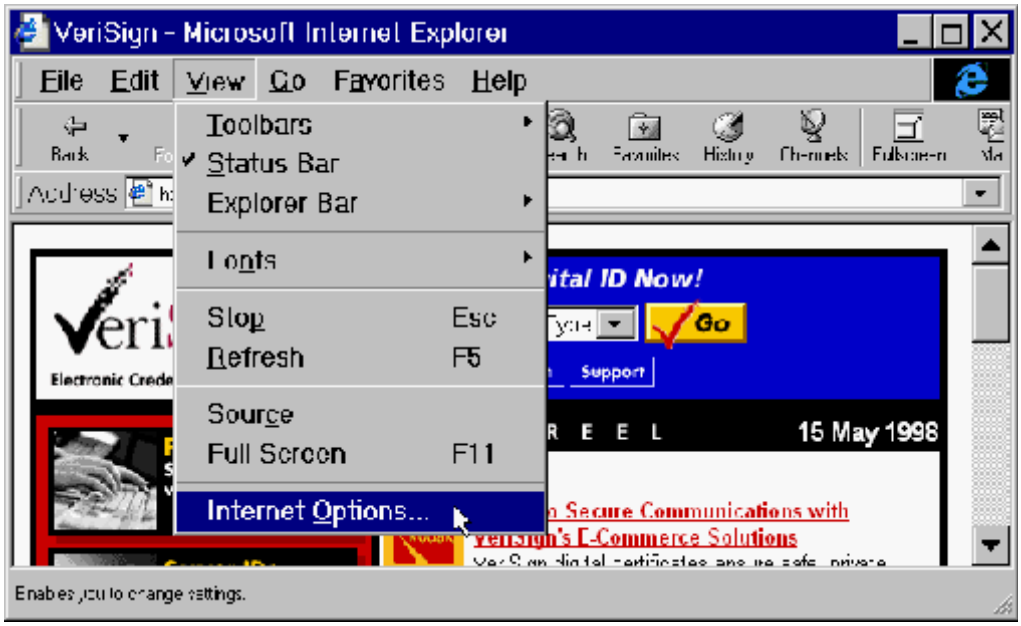

Figure 2-24: Microsoft Internet Explorer Menu Bar and Drop Down

Step 2: In the Internet Options window, click on the **Content** tab, select **Personal**, and click on the **OK** button.

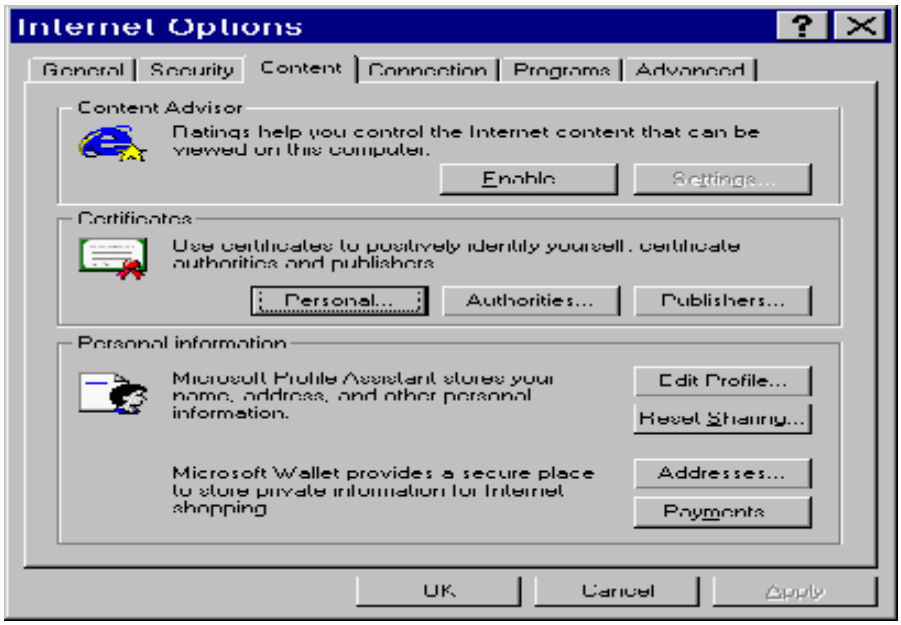

Figure 2-25: Internet Options Window

Step 3: The Client Authentication window appears. Highlight your **Digital ID** and click on **View Certificate**.

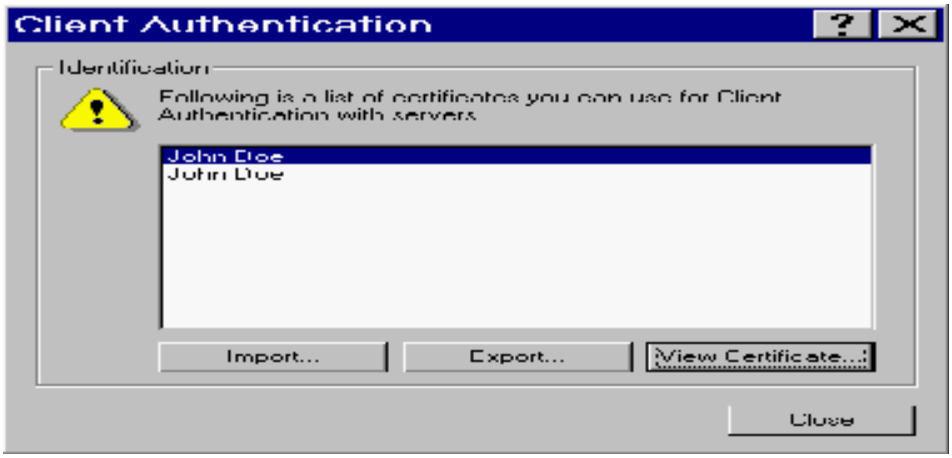

Figure 2-26: Client Authentication Window

Step 4: View the contents of your Digital ID in the Certificate Properties window that appears.

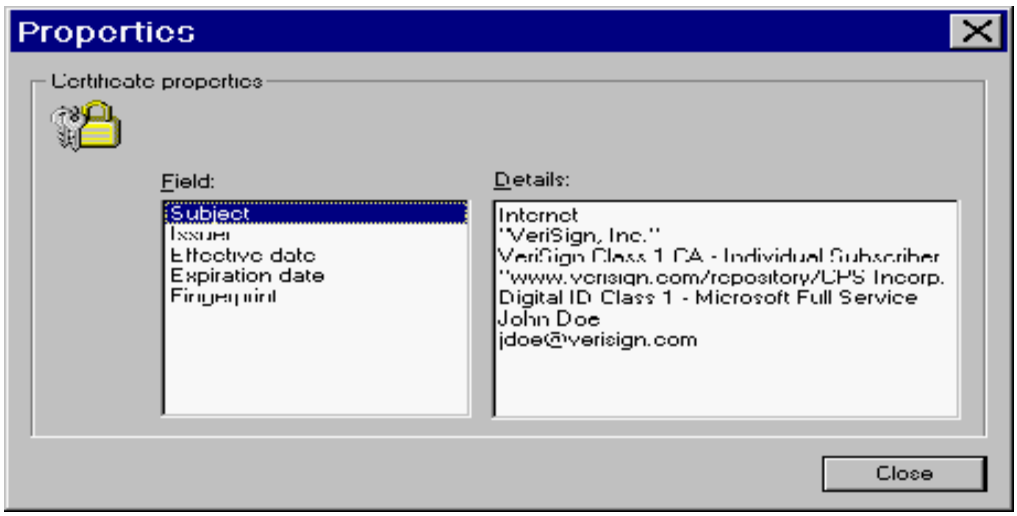

Figure 2-27: Microsoft Certificate Properties Window

If your Digital ID fails to appear as described above, you will need to return to the VeriSign Onsite host page and retrieve your certificate again. (See Section 2.5.) If this subsequent attempt fails, you will need to re-enroll. (See Section 2.2.)

2.7 Obtaining the Netscape Signaturing File

In order to sign or verify signatures, Netscape users will need to obtain a special digital signature file. The required file is named “DS_Netscape.ifx” and can be obtained via the NRC EIE home page. In order to obtain and install the Netscape signaturing file, follow the instructions below.

Step 1: Access the NRC EIE home page at http://www.nrc.gov./NRC/EIE/index.html. Click on the EIE Start Up hyperlink. Go to Step 2 and click on **Download the Plug-in** to download the Netscape signaturing plug-in for your browser.

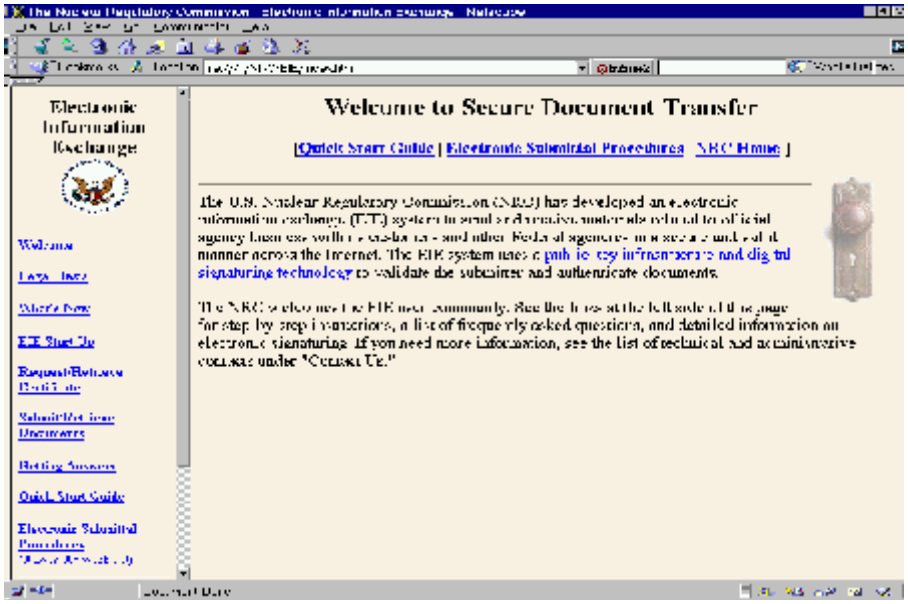

Figure 2-28: NRC EIE Home Page

Step 2: The EIE Quick Start page appears. Go to Step 2 and click on **Download the Plug-in** to download the Netscape signaturing plug-in for your browser.

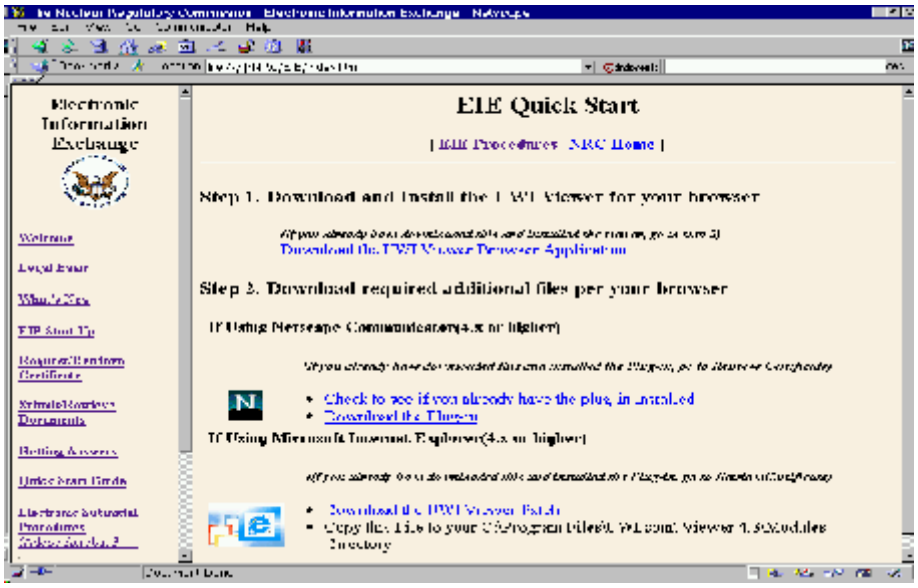

Figure 2-29: EIE Quick Start Page

Step 3: The **Save As** window appears. Navigate to Drive C:\ and to a temporary folder in which you wish to save the file, IFXNDSS.EXE. The download will take approximately one minute on average. Click on **Save** and return to the EIE home page.

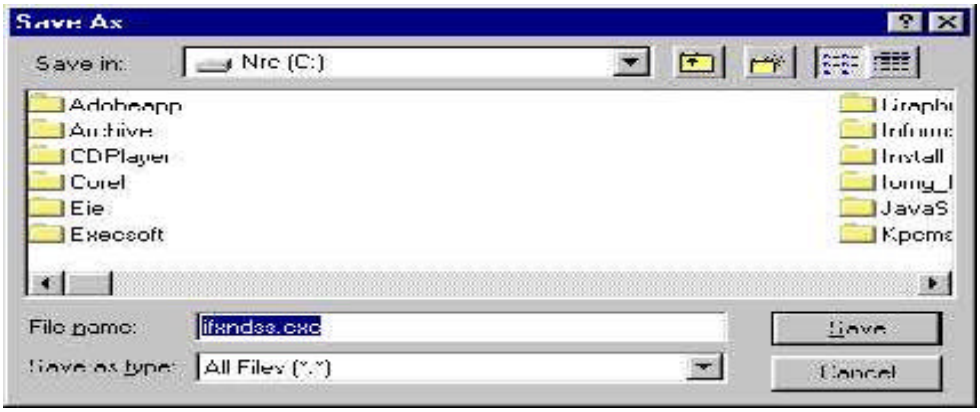

Figure 2-30: Save Netscape Signaturing File

Step 4: Close your Netscape browser and exit all other Windows applications before running the following setup programs. Access Drive C:\ and go to the temporary folder in which the plug-ins were saved. Install the InternetForms Extension for Netscape Digital Signature Support, IFXNDSS.EXE, by double-clicking the file icon. Follow the steps provided by the setup dialog.

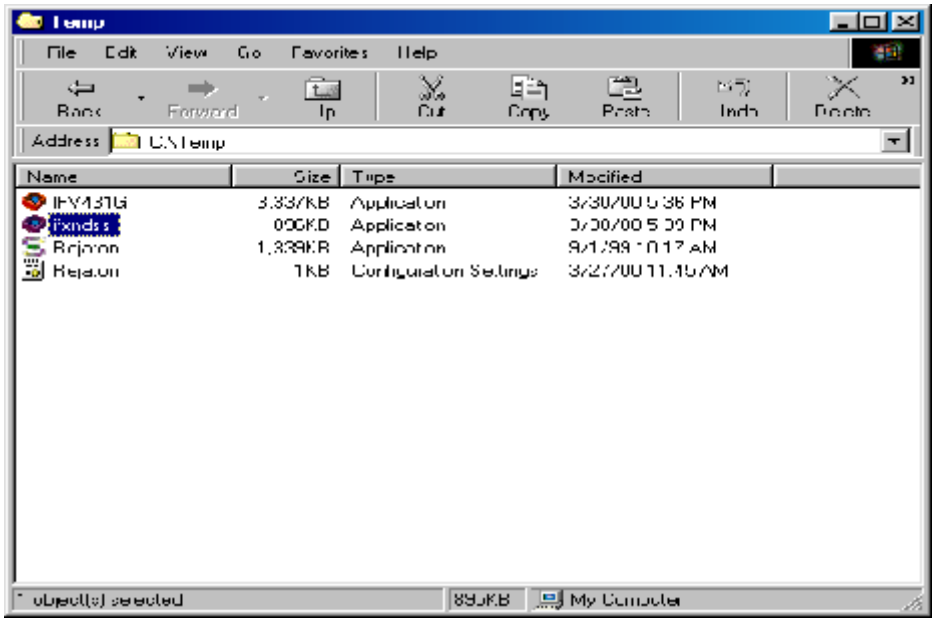

Figure 2-31: IFXNDSS.EXE File

Step 5: The install warning window appears.

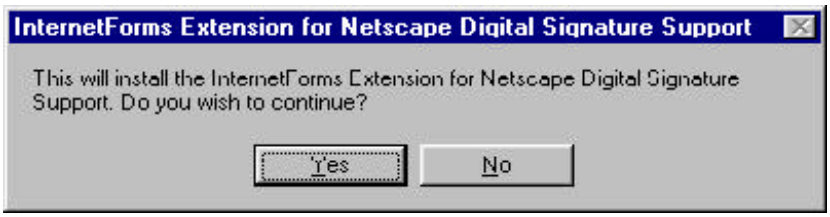

Figure 2-32: Install Warning Window

Click on the **Yes** button.

Step 6: The run setup window appears.

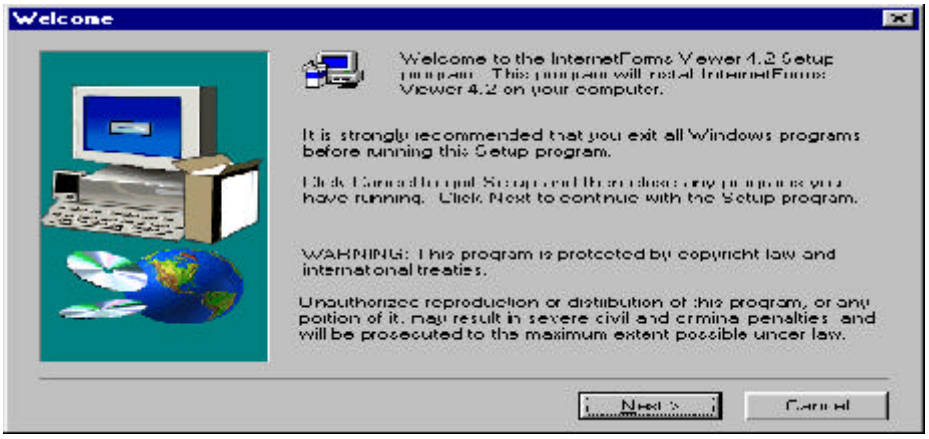

Figure 2-33: Run setup window

Step 7: Run setup by clicking on the **Next** button. The Software License Agreement window appears.

Figure 2-34: Software License Agreement

Click on the **Yes** button to continue setup.

Step 8: When the setup is complete, the Setup Complete dialog box appears.

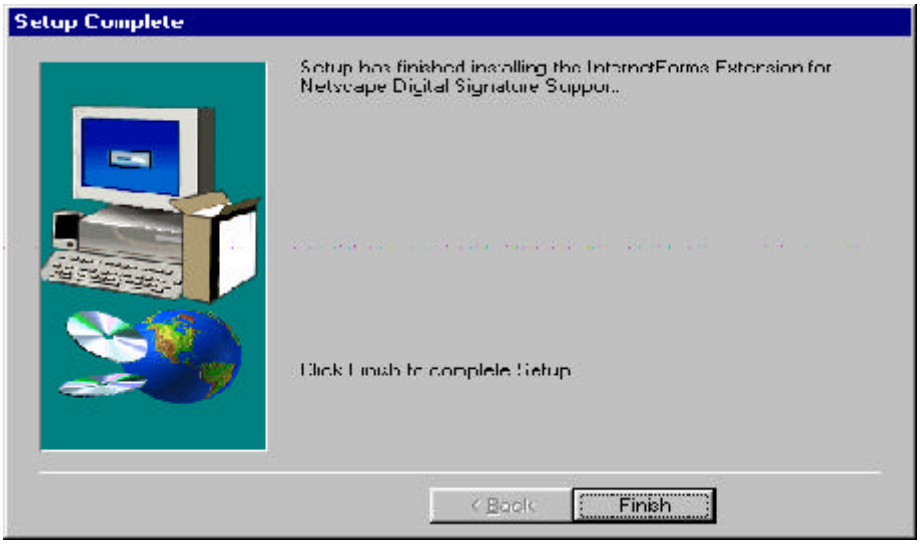

Figure 2-35: Setup Complete

Click on the **Finish** button.

Participants using Netscape are now able to use their Digital ID for signaturing.

2.8 Obtaining the InternetForms Viewer

In order to properly utilize the form, participants will need the InternetForms Viewer. The viewer is a program that enables the form to be opened and read. The latest version of InternetForms, can be downloaded from the NRC EIE home page. The process for downloading the viewer is detailed below.

Step 1: Access the NRC EIE home page at http://www.nrc.gov/NRC/EIE/index.html. Upon connection, the NRC EIE home page appears. Click on the EIE Start Up hyperlink.

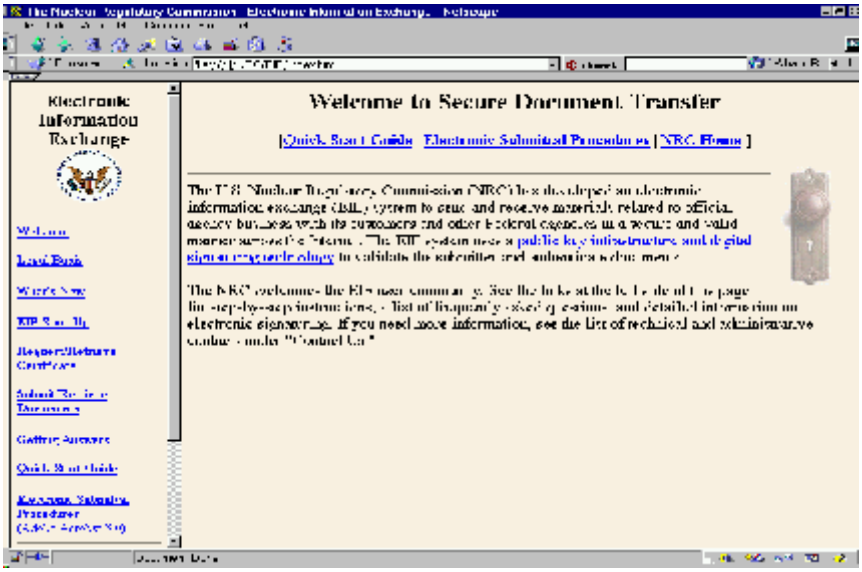

Figure 2-36: NRC EIE Home Page

Step 2: The EIE Quick Start page appears. Go to Step 1, "Download and Install the UWI Viewer for your browser." Click on **Download the Viewer Plug-in**.

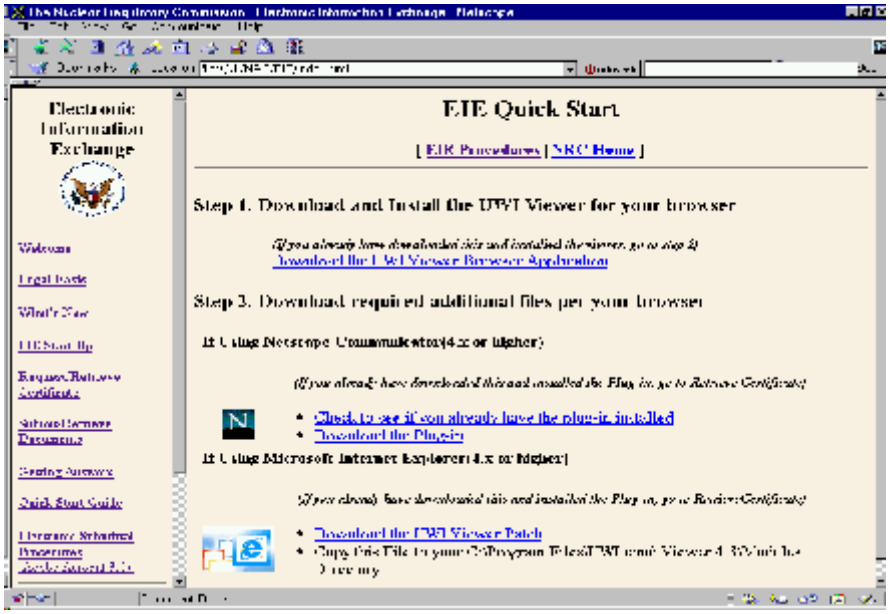

Figure 2-37: EIE Quick Start Page

The download process varies depending on which browser you are using. The process for both Netscape and Microsoft Internet Explorer are outlined below.

Netscape Navigator/Communicator (version 4.6 or higher)

Step 3: Netscape users will receive the viewer license agreement as shown below.

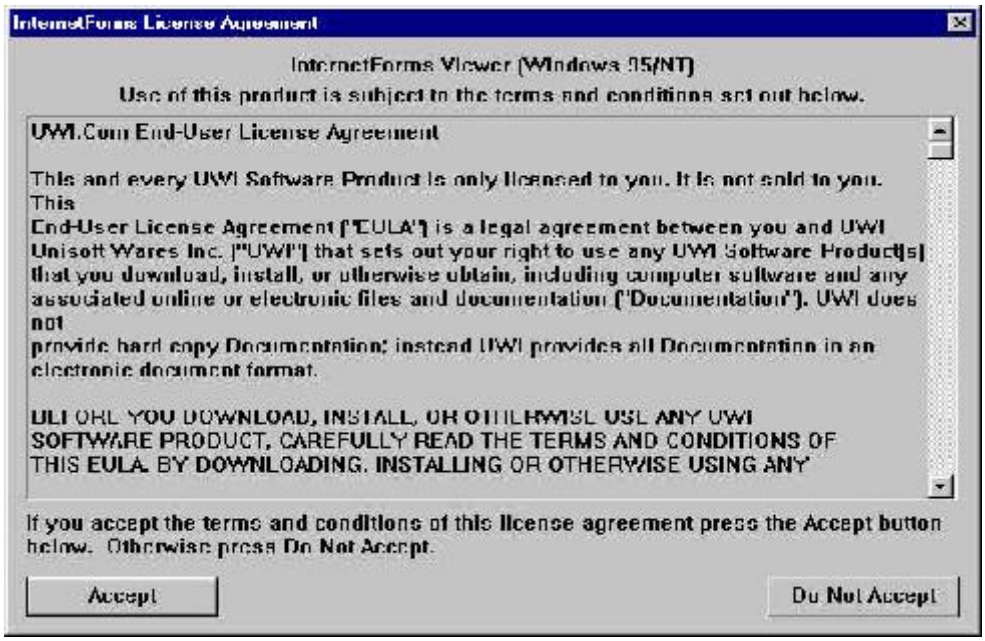

Figure 2-38: Viewer License Agreement

Read the viewer license agreement. If you accept the terms, click on **Accept** to begin the viewer download process.

Microsoft Internet Explorer (version 5.0 or higher)

Step 3a: Instead of the viewer license agreement, Internet Explorer users will receive the Save the file dialog as shown below.

Upon accepting the viewer license agreement or clicking on **Yes** to save the file, both Netscape and Internet Explorer users receive the save as dialog and the download and installation processes will proceed the same for each.

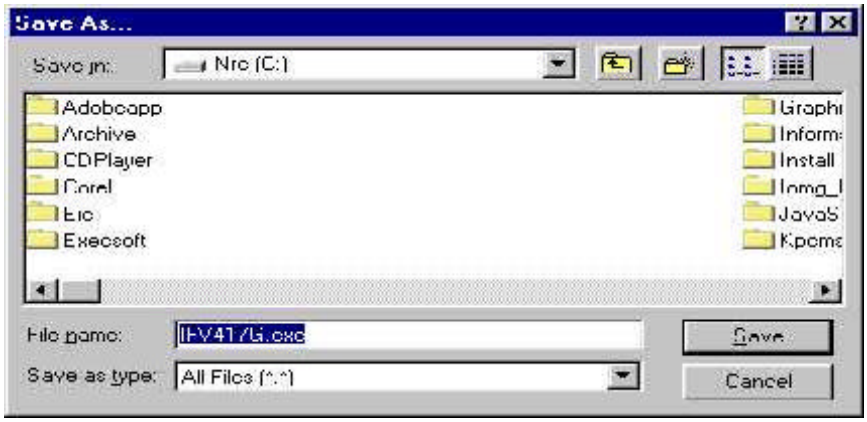

Figure 2-39: Save Form Viewer File

Step 4: From the Save As dialog, navigate to the appropriate drive and folder. (The default drive is C:\.) It is recommended that you save the file in a temporary (Temp) folder on your C:\ drive.

Step 5: Click on the **Save** button to save the downloaded file. Close the browser and install the viewer.

Installation:

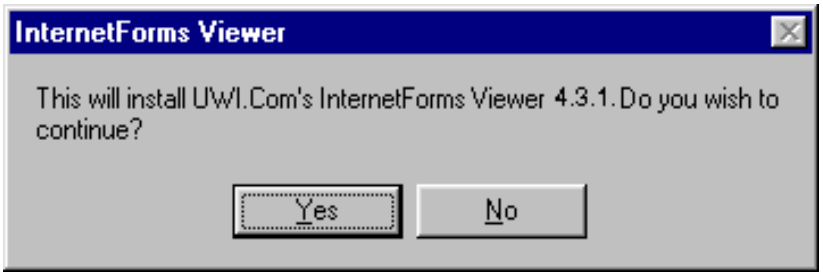

Figure 2-40: InternetForms Viewer Warning

Step 1: Navigate to the folder containing the downloaded file (file name, IFV431G.exe). Double click on the file icon.

Step 2: The InternetForms viewer warning appears.

Click on the **Yes** button to continue installation.

Step 3: The viewer setup begins and the Welcome window appears.

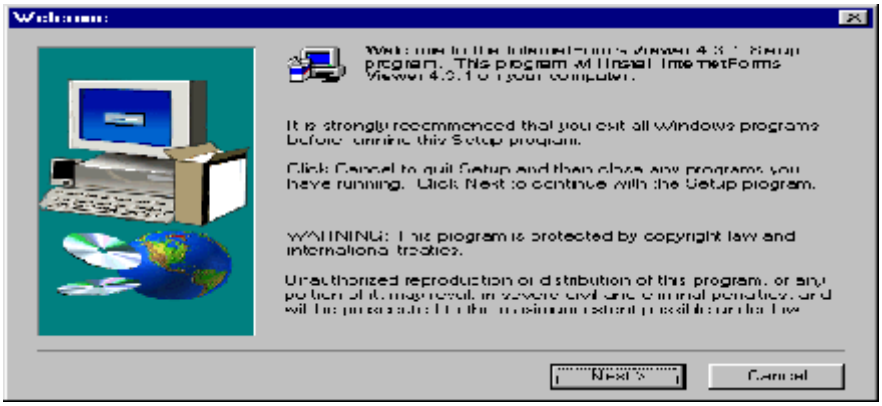

Figure 2-41: InternetForms Viewer Welcome Window

Click on **Next** to continue setup.

Step 4: The Software License Agreement dialog appears.

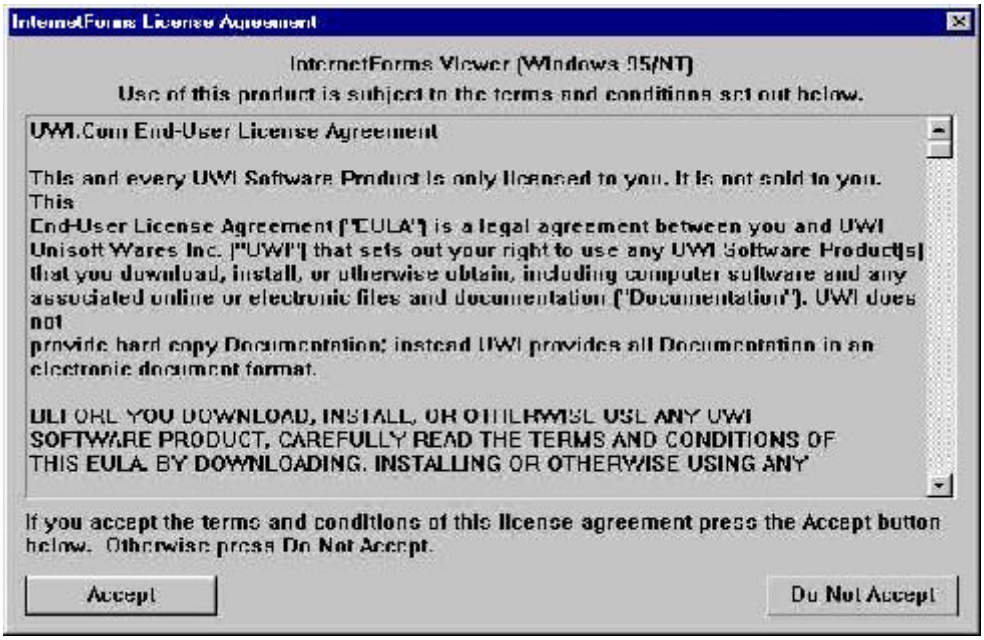

Figure 2-42: Viewer License Agreement

Read the agreement. If you accept all the terms, click on **Yes** to accept it and continue setup.

Step 5: Next, the User Information window appears.

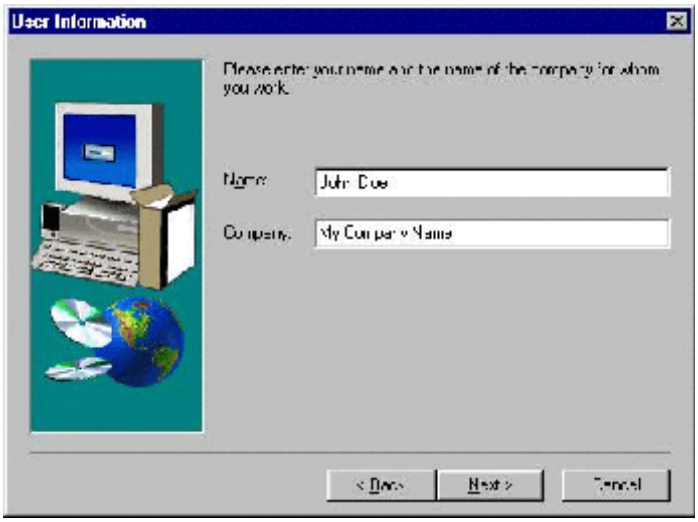

Figure 2-43: User Information Window

Enter user information, participant name and company (agency) name. Click on **Next** to continue.

Step 6: Choose a destination location for the installation. (Note: Setup automatically creates a destination location (folder), however, you may click on **Browse** and select a different one.)

Figure 2-44: Choose Destination Location

Click on **Next** when done.

Step 7: Select a program folder. It is recommended that participants use the default

folder, InternetForms Viewer 4.3.1.

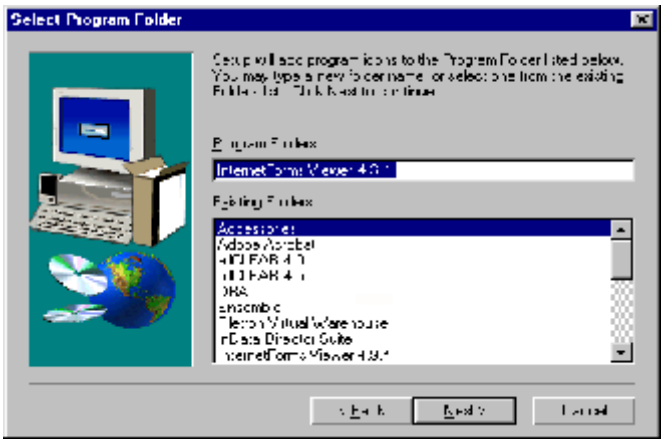

Figure 2-45: Select Program Folder

Click on **Next** to continue.

Step 8: Setup runs and the setup complete window appears when done.

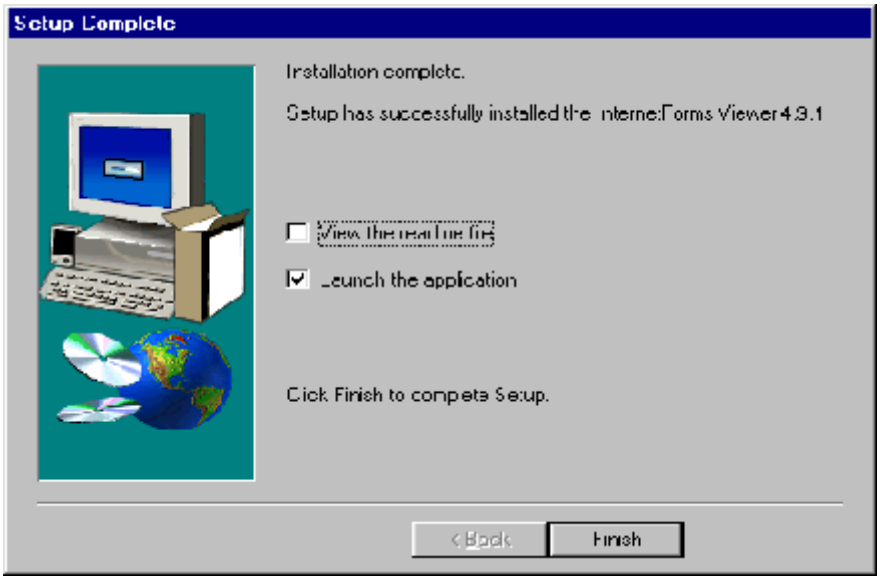

Figure 2-46: Setup Complete

Click on the **Finish** button to complete installation.

2.9 Providing Backup for Digital ID Certificates

EIE participants are responsible for the security of their own individual Digital ID certificates. In this regard, participants are encouraged to make a backup copy of their

Digital ID. The steps applicable to each browser are outlined below.

Netscape Navigator/Communicator (version 4.6 or higher)

Netscape users can accomplish this in the following manner.

Step 1: Open the Security Advisor/Info window and select **Yours** from the left hand margin under Certificates. Highlight the Digital ID for backup and click on the **Export** button.

Figure 2-47: Security Advisor/Window

Step 2: The Netscape Password Entry Dialog window appears. **Enter** your Netscape Certificate Database password. You will be prompted to specify another password to protect your Digital ID export file. **Confirm** the export file password a second time. Click on the **OK** button.

Figure 2-48: Password Entry Dialog

Step 3: The File Name to Export window appears. Name the file. The Digital ID is saved with a ".p12" file extension. It is recommended that you save your Digital ID on diskette and store the diskette in a safe and secure place. Click on the **Save** button.

Figure 2-49: File Name to Export Window

Step 4: A confirmation message appears when the Certificate has been successfully exported.

Figure 2-50: Successful Export Message

Microsoft Internet Explorer (version 5.0 or higher)

Step 1: Select **View** from the menu bar and click on **Internet Options** on the drop down menu.

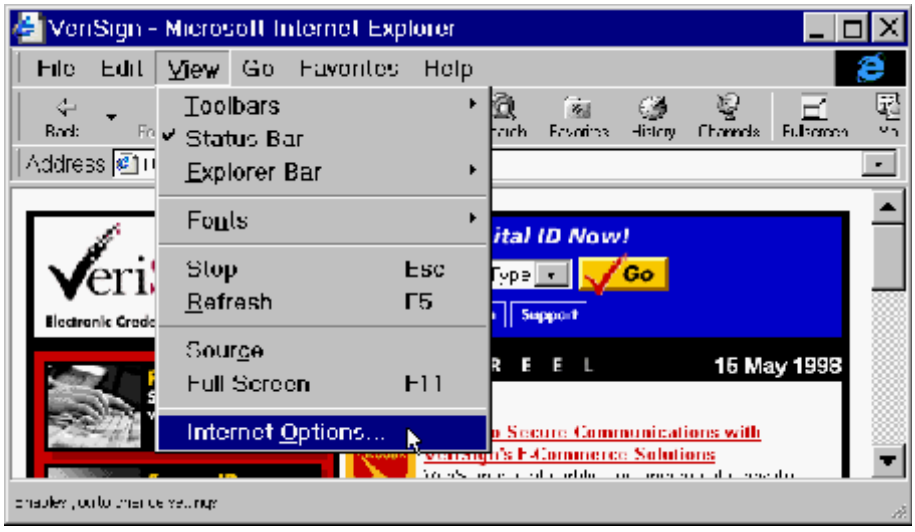

Figure 2-51: Microsoft Menu Bar and Drop Down

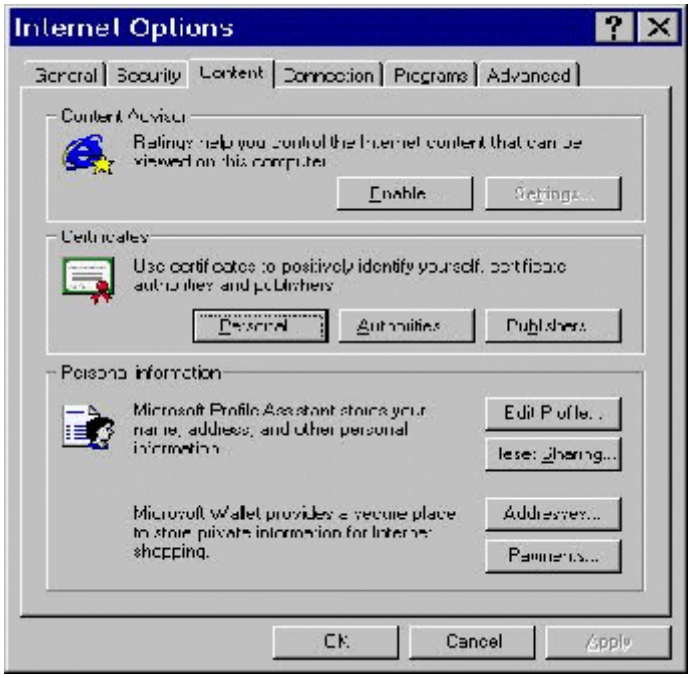

Figure 2-52: Internet Options Window

Step 2: In the Internet Options window, click on the tab labeled **Content**, click on the **Personal** button, and then click on the **OK** button.

The Client Authentication window appears.

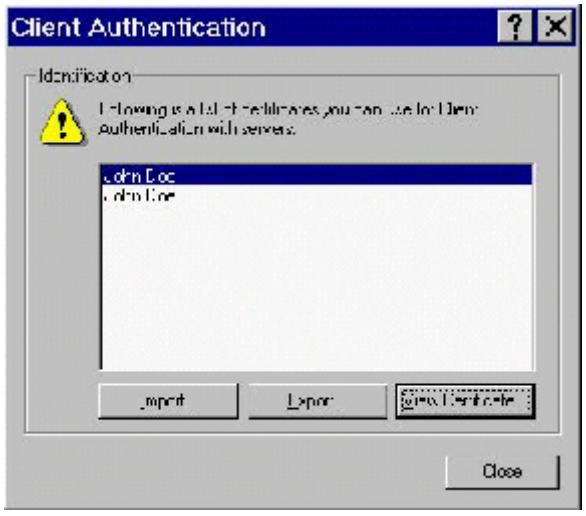

Figure 2-53: Client Authentication window

Step 3: Select and highlight the **Digital ID** to be exported. Click on the **Export** button. The Export Personal Certificates window appears.

Figure 2-54: Export Personal Certificates Window

Step 4: In the Export Personal Certificates window, enter and confirm the password to be used to protect this file. Specify using a ".pfx" extension. Click on the **OK** button.

2.10 Replacing Digital ID Certificates

If the backup Digital ID certificate becomes misplaced, lost, or compromised, participants must revoke and replace their certificate and replace it. In the case of a lost, misplaced, or possibly compromised Digital ID certificate, participants should follow these steps to replace it.

Step 1: Access the enrollment page at the following URL: https://onsite.verisign.com/USNuclearRegulatoryCommissionADDOCIO/index.html. Or, go to the NRC EIE Home page and click on the Request/Retrieve Certificate hyperlink. From the Request/Retrieve Certificate page, click on the **Go to the VeriSign/NRC Page** hyperlink.

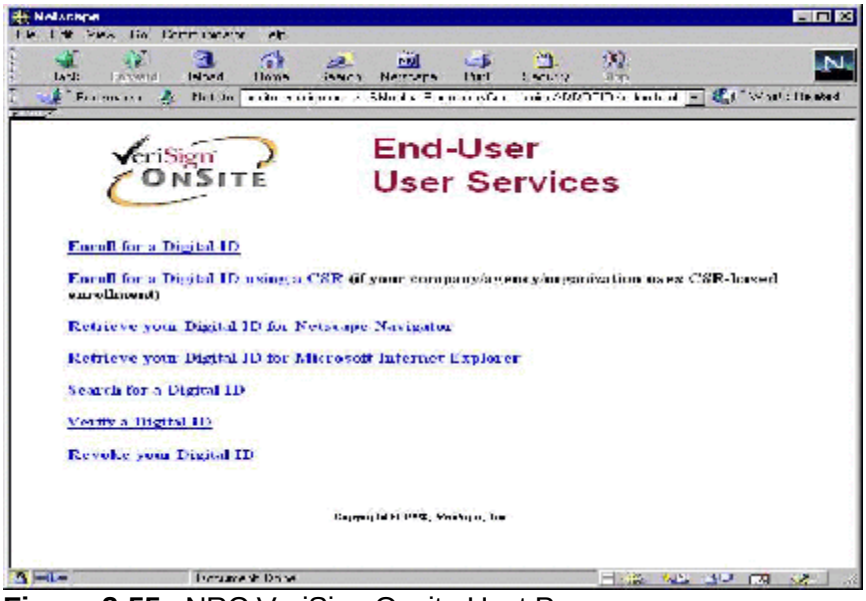

Figure 2-55: NRC VeriSign Onsite Host Page

Step 2: Select the last option listed, **Revoke your Digital ID**. The Digital ID Search window appears.

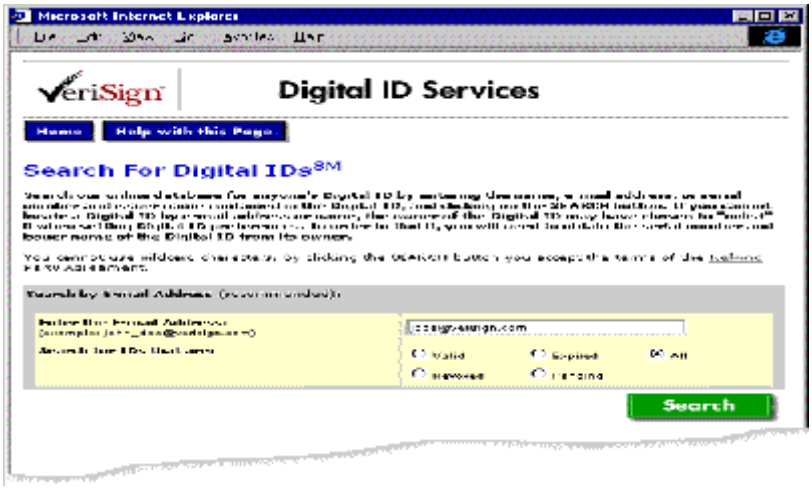

Figure 2-56: Digital ID Search Window

Step 3: You will be prompted to search for the Digital ID. Enter you e-mail address to search for it. When the search is done, the result is displayed as follows.

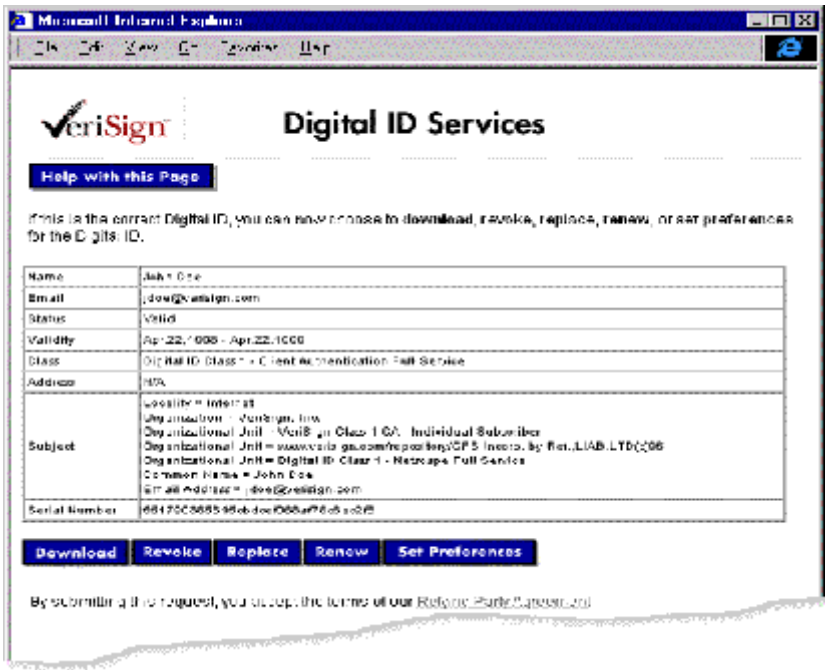

Figure 2-57: Digital ID Listed

Step 4: Click on the **Replace** button. The Revoke and Replace Your Digital ID window appears.

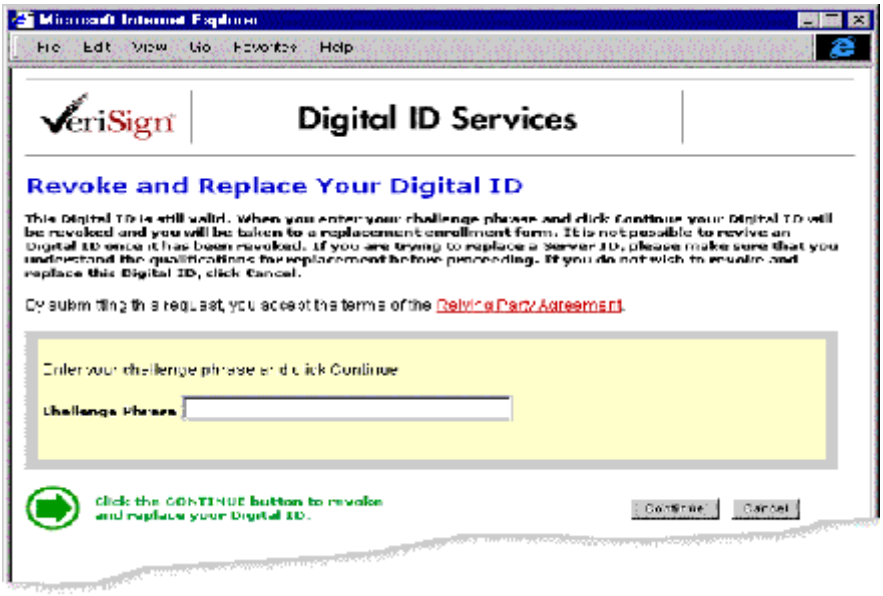

Figure: 2-58: Replace Digital ID Window

Step 5: Identify yourself by entering your "Challenge Phrase." Click on the **Continue** button to revoke your certificate and generate a new one.

Once the request for revocation and the issuance of a new Digital ID is complete, the new private key is generated and the request is forwarded to the LRA for action. From this point, the same processes outlined in sections 2.3 and 2.4 apply.

2.11 Replacing Netscape Digital ID Certificate Passwords

In the case of not being able to recall your password, Netscape users may replace their password as long as a copy of the Digital ID Certificate is on a diskette or the hard drive. If you do not have a copy of your Digital ID Certificate, you will not be able to replace your password, but rather follow the steps outlined above to replace the Digital ID. If you have a copy of your Digital Certificate, follow the steps below.

Step 1: Open Windows and locate the cert7.db file using Windows Explorer.

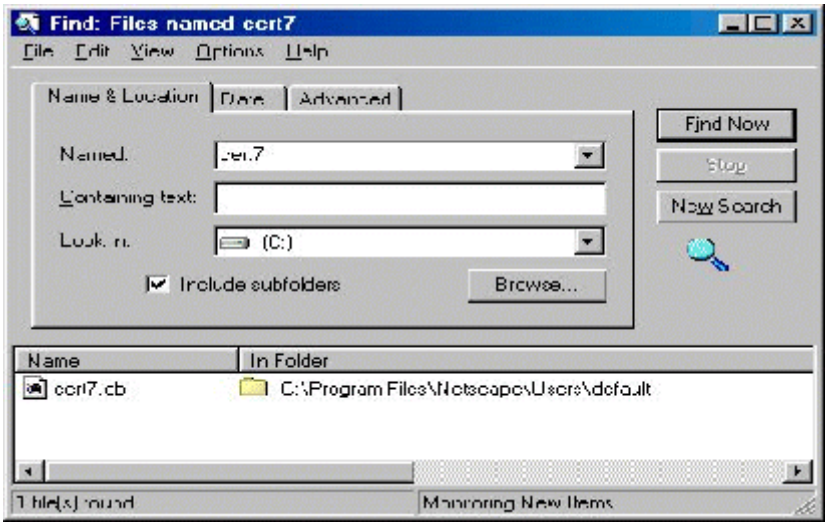

Figure 2-59: Files named cert7.db in Windows explorer

For Windows 95/97/98 users, the file should be located in C:\Program Files\ NETSCAPE\Users\your_name.

Step 2: Once located, delete the cert7.db file.

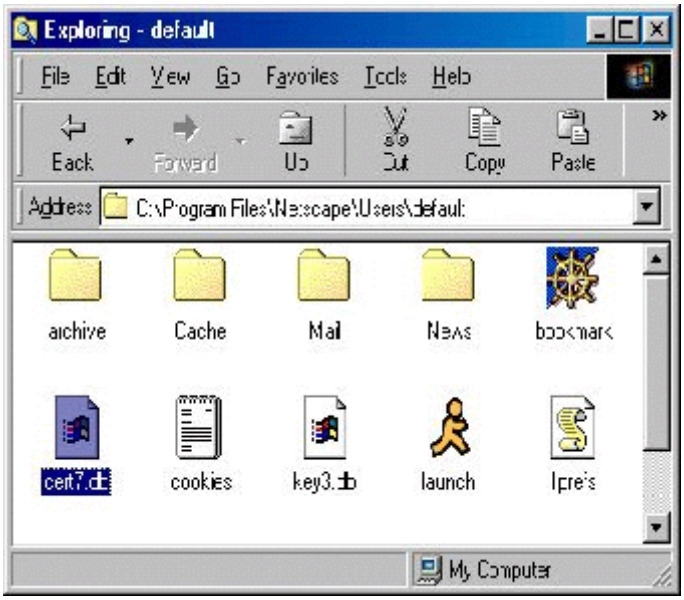

Figure 2-60: Delete certificate window

Step 3: Open your browser and click on the Security icon to open the Security Advisor/Info window.

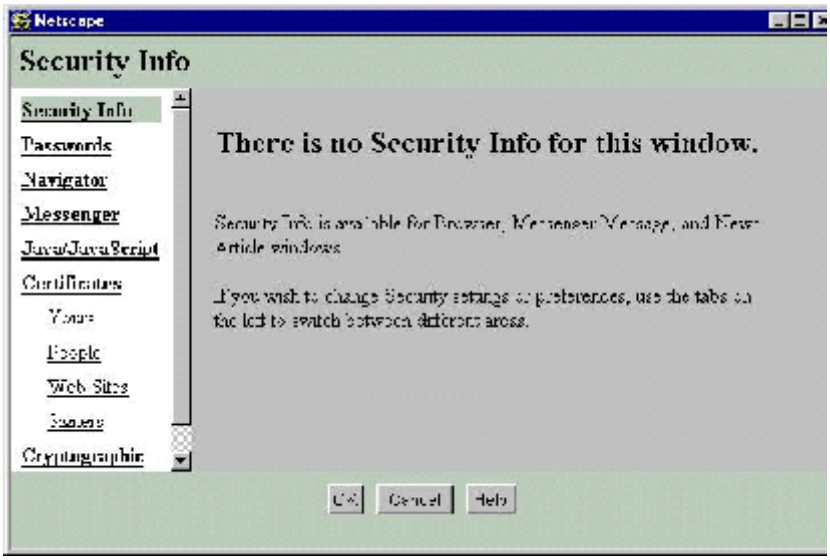

Figure 2-61: Security Advisor/Info Window

Step 4: In the Security Advisor/Info window, select **Yours** under Certificates.

Step 5: From the certificates window, highlight your certificate and click on the **Delete**

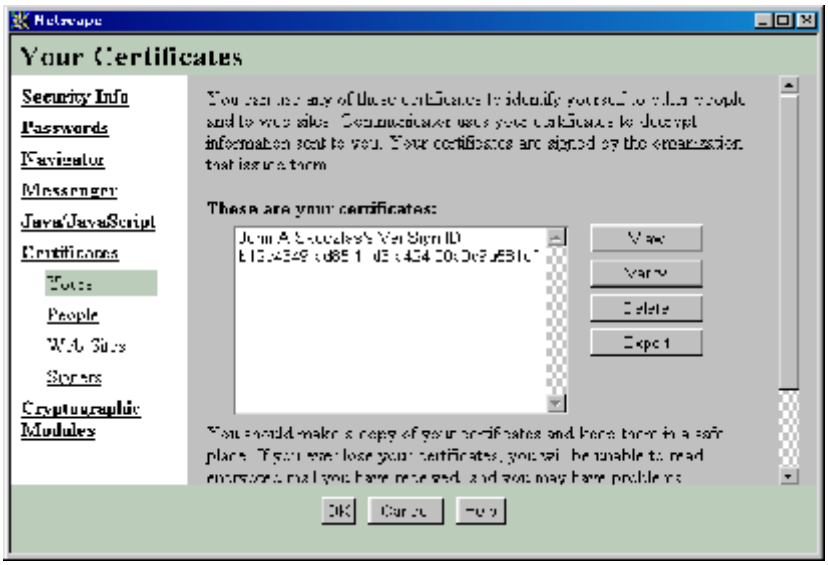

Figure 2-62: Your Certificates in Security Advisor/Info window

button. This will delete your certificate from your browser.

Step 6: Close your browser and restart Windows. Once windows has restarted, open your browser. Click on the **Security** icon to open the Security Advisor/Info window.

Step 7: In the Security Advisor/Info window, select **Passwords**. Click on the **Set**

Password button to create a new password.

Figure: 2-63: Set Password

Step 8: After creating a new password, select **Yours** under certificates. Use the right-hand scroll bar to scroll to the bottom of the certificates window. Click on **Import a Certificate**. Insert the diskette containing your certificate in drive A: or wait for the prompt to navigate to drive C: (if your certificate is saved there).

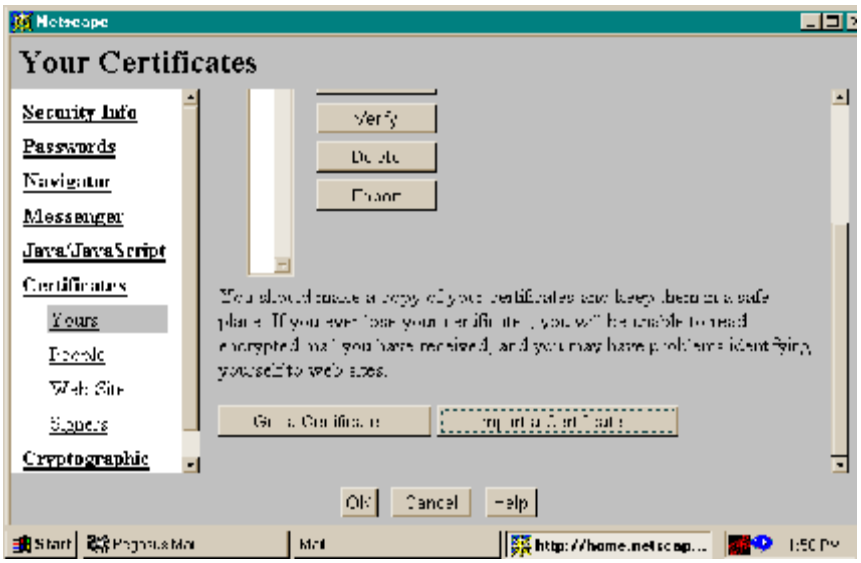

Figure 2-64: Import a Certificate

Step 9: This invokes the Password Entry Dialog. Enter the new password and click on **OK**. This opens the File Name to Import window.

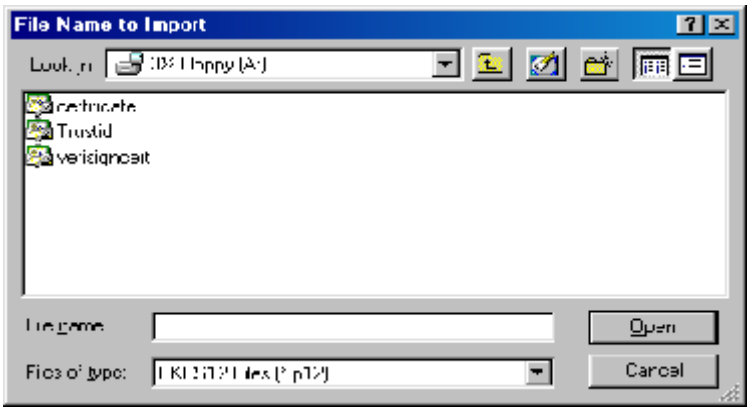

Figure 2-65: File Name to Import Window

Step 10: Insert the diskette containing your certificate in drive A: or wait for the prompt to navigate to drive C: (if your certificate is saved there). Locate the certificate and begin the import process by either double clicking on the certificate icon or by highlighting it and clicking the **Open** button.

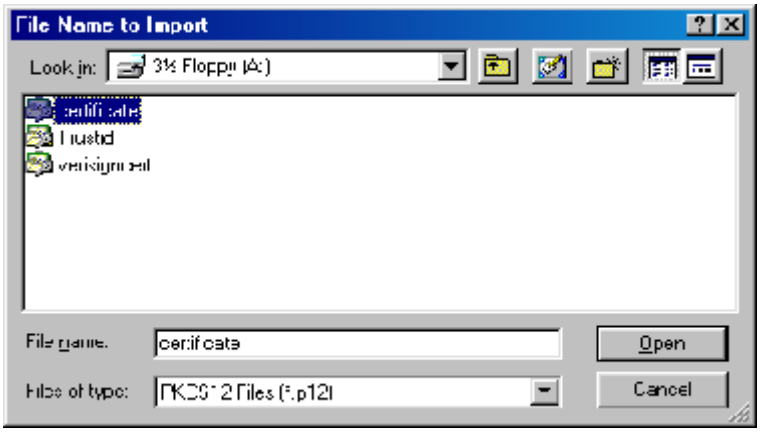

Figure 2-66: File Name to Import Window

Step 11: The Password Entry Dialog now opens. Enter the password for the file to be imported. (This is the password assigned when the certificate was first backed-up. See Section 2.8). Click on the **OK** button.

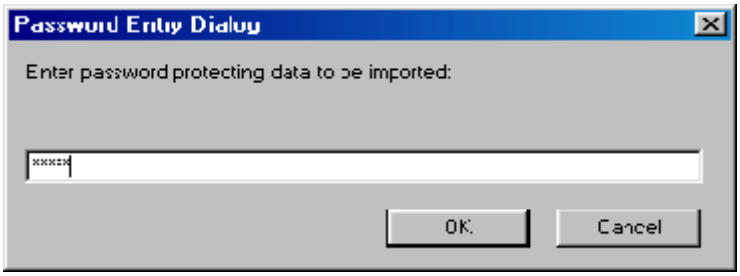

Figure 2-67: Password Entry Dialog

Step 12: Netscape then displays a message stating that the certificate has been successfully imported.

Figure 2-68: Successfully Imported Certificate

Click on the **OK** button. Return to the Security Advisor/Info window and exit the browser. Once the certificate has been successfully imported, you may use it again in conjunction with your new password.

3.0 HOW TO SUBMIT DOCUMENTS

3.1 Introduction

Documents eligible for submission to the NRC or for transmission from the NRC are restricted to specific formats. The acceptable formats for electronic submittal are Portable Document Format (PDF) Normal versions 3.0 or 4.0, PDF Image plus Hidden Text versions 3.0 or 4.0, ASCII, Multi Page TIFF, Word Perfect 6/7/8, Corel Presentations, Quattro Pro, MS Word 95/97, MS Excel 95/97, and MS Powerpoint 95/97. **The preferred formats are PDF plus Hidden Text, PDF Normal and Multi Page TIFF.** If Multi Page TIFF formatted documents are submitted, the resolution must be as follows:

- bitonal (black and white) TIFF resolution - 300 dpi
- color TIFF resolution - 150 dpi
- grayscale TIFF resolution - 150 dpi

Participants shall use the NRC EIE Form (form) to submit or transmit documents. The form shall contain, as an enclosure, the document(s) to be submitted or transmitted. In addition, each form submitted must be digitally signed. In order to open and read a form, each participant shall require a form viewer. The steps necessary to perform each of these processes are described in the following sections.

3.2 How to Obtain the NRC EIE Form

The submission or transmission of EIE documents will require the use of the NRC EIE form. The EIE form is an intelligent document based on Extensible Machine Language (XML). It allows participants to sign, enclose, submit, and verify documents via the Internet. Participants may choose to simply access the form via the NRC EIE home page each time they wish to submit a document. Similar to the viewer, the form can be obtained by following the steps outlined below.

Step 1: Access the NRC EIE home page at http://www.nrc.gov/NRC/EIE/index.html. Once connected, click on the **Submit/Retrieve Documents** hyperlink. From the Submit/Retrieve Documents page, click on **Go to the NRC Form** under Step 6.

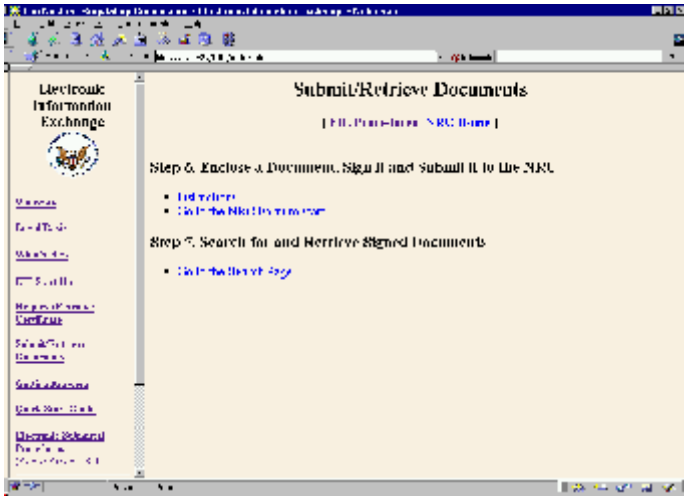

Figure 3-1: Submit/Retrieve Documents Page

Step 2: The "Select a Certificate" window appears. (Note: In order to access the EIE server and retrieve documents, each participant must have an NRC issued Digital ID certificate).

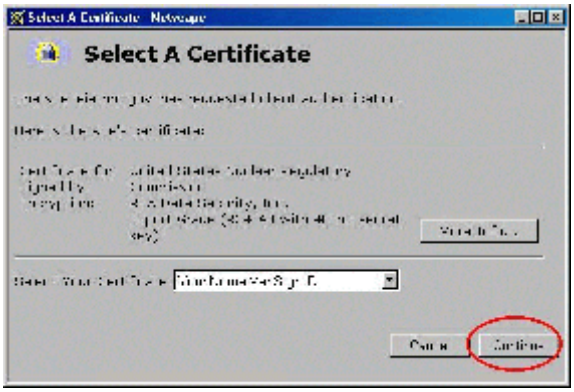

Figure 3-2: Select a certificate

Select your NRC issued certificate and click on the **Continue** button. The Password Entry dialog appears.

Figure 3-3: Netscape Password Dialog Box

Step 3: Enter your password for the Certificate Database and click on **OK**. You will be prompted to re-enter it for confirmation, click on the **OK** button. A Security Information window appears, click on **Continue**.

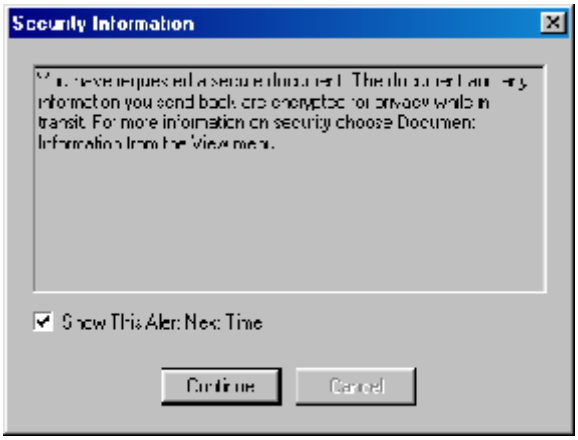

Figure 3-4: Security Information Window

Step 4: The Security Warning window appears. Click on **OK** to continue.

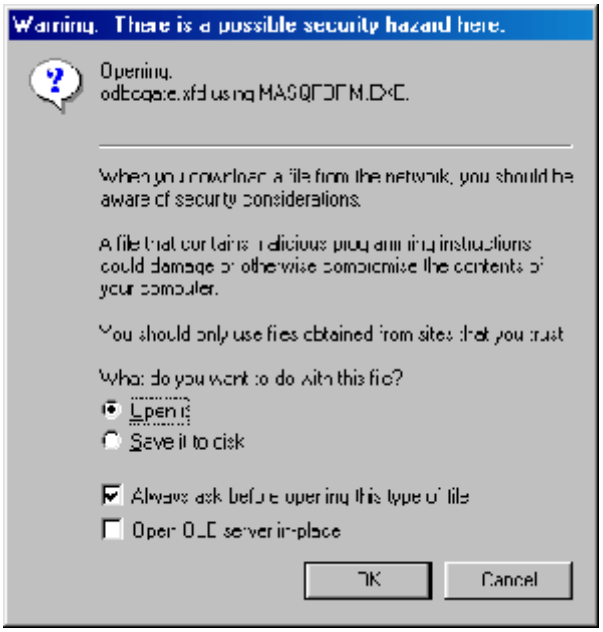

Figure 3-5: Security Warning Window

The PureEdge InternetForms viewer is loaded and the NRC EIE Form is displayed.

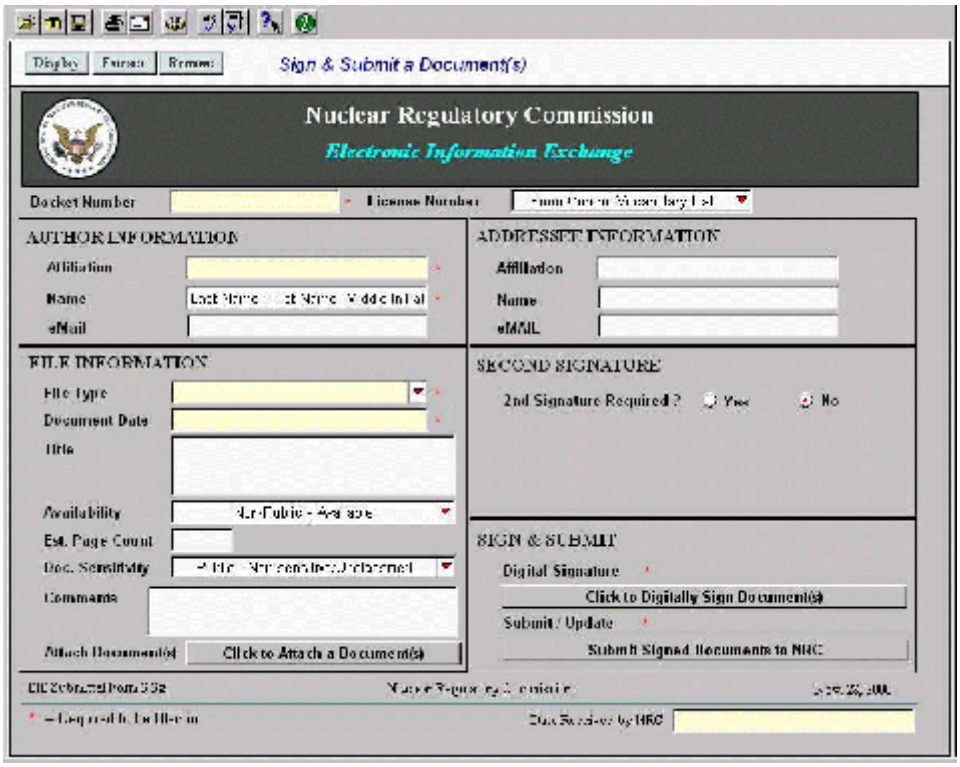

Figure 3-6: NRC EIE Form

Step 5: If you wish to download the form, select **File** from the browser's menu bar and click on **Save As**. This invokes the Save As dialog box.

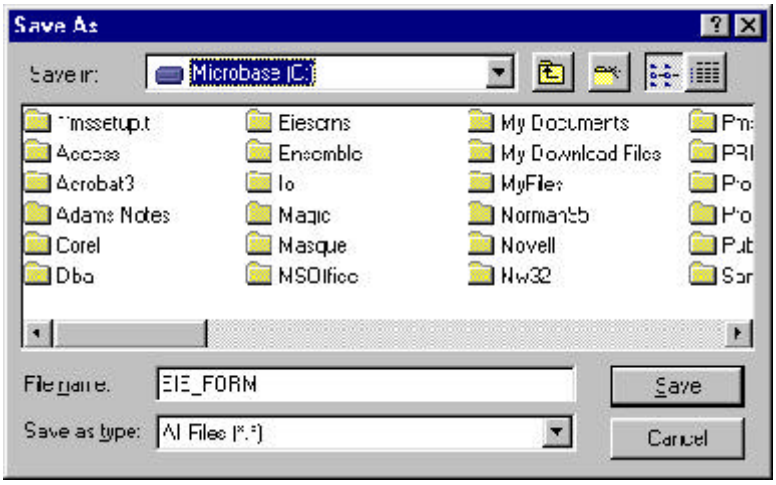

Figure 3-7: Save as Dialog Box

Step 6: Select the drive and directory in which you wish to save the form and click on the **Save** button. (The default drive is the C:\ drive.)

3.3 How to Complete the Form

The NRC EIE form contains several fields for bibliographic information. The form's bibliographic fields are listed and described in Table 3-1 below.

Field Name	Description	Required Y/N
Docket Number	The document's NRC docket number(s), i.e., 50-424 and/or 50-425.	Y
License Number	NRC assigned license number.	Y
Author Affiliation	The agency, department, or company name of the document's author.	Y
Author Name	The author(s) of the document(s).	Y
Author/Submitter E-Mail	E-mail address of author or submitter.	Y
File Type	The document's file type, i.e., "Adobe PDF," or Corel WordPerfect 6/7/8.	Y
Document Date	The date of the Form Submittal.	Y
Title	Title of the enclosed document(s).	Y
Availability	Designation whether document(s) is publicly or non-publicly available.	Y
Estimated Page Count	Approximate number of pages of the submitted document(s).	Y
Document Sensitivity	Designation of document(s) level of sensitivity, i.e. Public - Nonsensitive/Unclassified.	Y
Comments	General notes pertaining to the document(s).	N
Addressee Name	Name(s) of those to whom the document(s) is addressed.	Y
Addressee Affiliation	Name of the organization to whom the document(s) is addressed.	Y
Addressee E-Mail	E-mail address(es) of those to whom the document(s) is addressed.	Y
Document Date Received	Date and time submittal is received by the NRC EIE server. This is entered programmatically by the server.	N

Table 3-1: NRC EIE Form Bibliographic Fields

Information must be entered into all fields with the exception of the “Comments” field which is optional. The required fields are denoted on the form by a red (*). Participants should take care to ensure that these fields are complete before attempting to submit the form. If an attempt is made to submit where any of these fields are left blank, the form’s submit function will not activate and the field(s) with missing information will be highlighted. This process interruption will occur until the empty fields are filled.

Documents submitted to the NRC should be addressed as follows:

ADDRESSEE INFORMATION

Affiliation	U.S. Nuclear Regulatory Commission
Name	Document Processing Center
Email	DocProcessingCenterX@nrc.gov

Upon completion of the bibliographic information, the form should look similar to the one below.

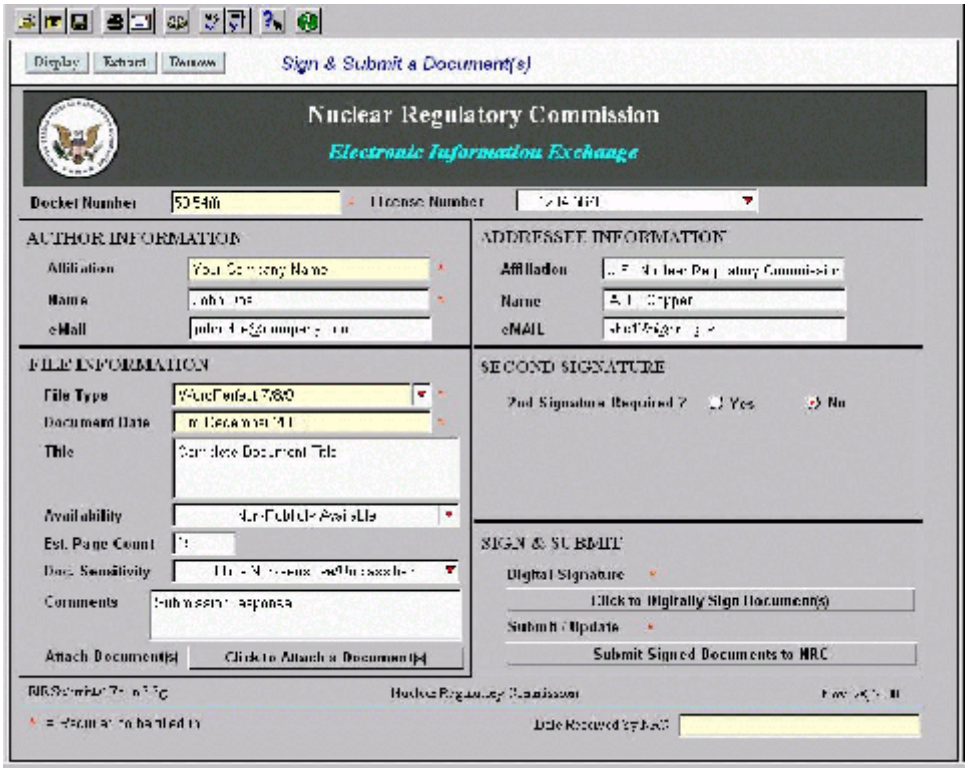

Figure 3-8: Completed NRC EIE Form

3.4 How to Enclose Documents

Once the viewer has been downloaded and installed, participants can utilize the form to collect documents for submission or transmission. This process is called enclosing or attaching documents. Each submittal shall be comprised of two parts, the EIE form and the documentary material(s) for submission. The contents of a form package consists of the collection of documentary material(s). Participants can enclose or attach documents by following the steps below.

Step 1: With the form open, click on the **Click to Attach a Document(s)** button. The Enclosures Dialog box appears.

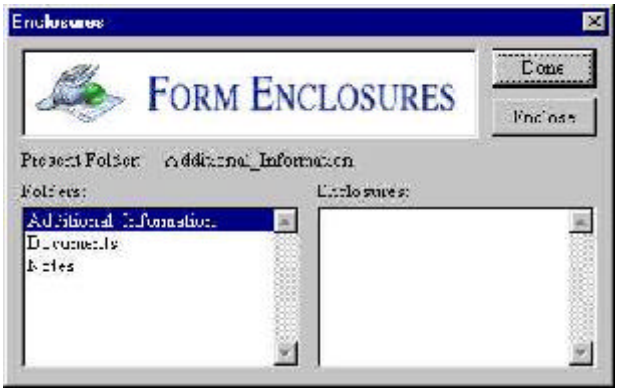

Figure 3-9: Enclosures Dialog Box

The Enclosures dialog box displays three folders on the left side. The “Documents” folder is used for documents, the “Additional Information” folder is used for supporting information, and the “Notes” folder is used for comments or notes. Select the “Documents” folder to enclose your document(s) by highlighting it.

Step 2: Click on the **Enclose** button in the upper right corner of the dialog box. This opens the Enclose File window that allows you to browse your drives and find the document(s) you wish to enclose.

Figure 3-10: Enclose File Window

Step 3: Within the window, navigate to the document to be enclosed. Select the document or file and enclose it by double clicking on it or by clicking to highlight it and then clicking on the **Open** button.

Step 4: After selecting the document or file, the Enclosures dialog box re-appears. The name of the chosen document or file appears in the enclosures directory on the right side of the dialog box with it's native application extension as shown below.

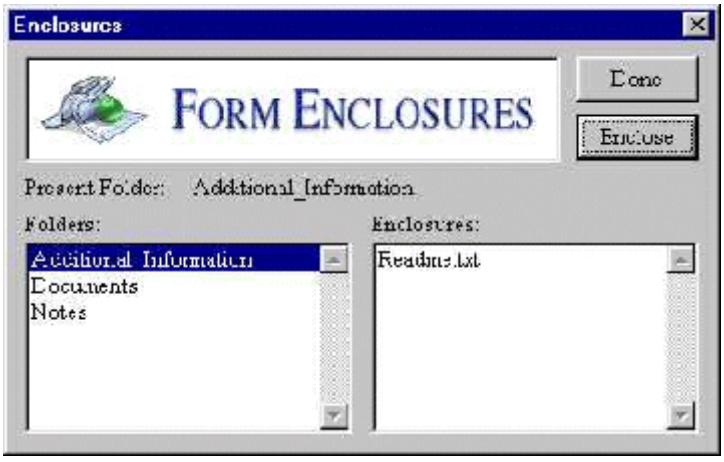

Figure 3-11: Form Enclosure Window

Step 5: To add additional documents or files for enclosure, repeat steps 2 and 3. When all necessary documents or files have been enclosed, click on the **Done** button.

There is no limit to the number of documents that can be enclosed. However, the file size for submittals is restricted to no more than 15 MB including the form which is approximately 40-50 KB.

After enclosing the document(s) necessary for submission, the form and its contents are ready for signing.

3.5 How to Sign (or Unsign) Forms

All documents submitted or transmitted shall be signed using digital signature software. The digital signature provides for the authentication, certification and security of documents submitted electronically. The submittal form provides for multiple signatures. However, documents that are submitted electronically do not necessarily have to be signed by the author. The document may be signed by the person who dispatches it as part of the transmittal process. Generally, those individuals who will digitally sign documents and submit them electronically to the NRC are the ones who currently dispatch licensing related materials to the NRC. Nevertheless, the author is accountable for the content of the document.

NRC regulations require that some submissions be made under oath. If such documents are transmitted electronically, the document must include, at an appropriate place, a statement substantially in this form:

> "I declare under penalty or perjury that the foregoing is true and correct to the best of my knowledge. Executed on (date)."

The electronic document **must** be digitally signed by the individual affirming the above statement. The individual affirming the above statement may then submit the document directly to the NRC using the EIE process or after digitally signing the affirmation, the individual may forward the signed document to another for dispatch to the NRC. If the document is forwarded for dispatch a second digital signature is required from the person actually sending the document to the NRC.

The form contains a signature field designed to allow participants to digitally sign a submittal. If a second signature is required, a second signature field is contained on the form to accommodate this. Once the bibliographic information has been completed and the necessary documents enclosed, participants can sign the form by following the steps outlined below.

Step 1: With the completed form open, click on the **Click to Digitally Sign Document(s)** button. Upon doing so, the Digital Signature Viewer dialog box appears.

The Digital Signature Viewer displays the caption "No Signature." This indicates that the form has not been signed. If you have a Digital ID Certificate, the **Sign** button is highlighted.

Figure 3-12: Digital Signature Viewer Dialog Box

Step 2: Click on the **Sign** button. The form will attempt to look up your Digital ID Certificate.

Step 3: At this point, Netscape users are asked for the password to their Certificate Database.

Figure 3-13: Netscape Password Window

Enter password and click on the **OK** button.

This initiates the signaturing process that retrieves the Digital ID Certificate stored in the browser. If successful, the viewer displays information pertaining to the signer such as the signer's name and e-mail address, the signature's hash algorithm, the certificate chain stating the name of the certificate authority that provided the signature certificate, and the class of certificate as illustrated below.

Figure 3-14: Digital Signature Viewer Dialog for Valid Signature

The viewer caption now changes to "Signature Is Valid."

Step 5: Sign the form by clicking on the **OK** button. The NRC EIE Form appears.

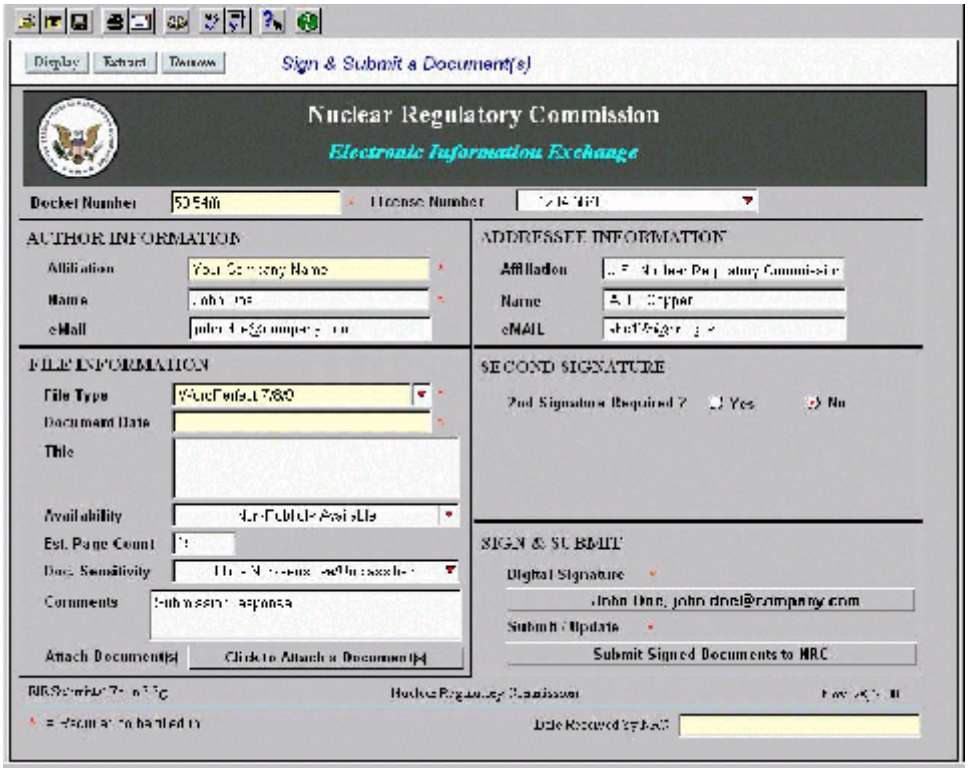

Figure 3-15: Signed NRC EIE Form

The “Digital Signature” field on the form now displays the signer’s name and e-mail address. After signing the form, it is ready to be submitted. Once the form is signed, it cannot be altered or modified. However, should a situation arise wherein a form is signed prematurely and additional material needs to be enclosed or material needs to be removed, the signature can be deleted to allow modification of the form’s contents. To accomplish this, apply the following steps.

Step 1: Click on the **Click to Digitally Sign Document(s)** button on the form. This produces the Digital Signature Viewer.

Figure 3-16: Digital Signature Viewer

Step 2: The **Delete** button is highlighted. Click on the **Delete** button. This removes the signature.

Once the signature is removed, the form and its contents can be altered or modified as needed. When the necessary modifications are complete, the form should be re-signed.

3.6 How to Submit/Transmit Documents

Documents submitted to the NRC or transmitted from the NRC shall be deposited on the NRC EIE external server for retrieval. The external server exists outside the NRC firewall. In order to submit a form and its contents to the external server from a workstation, participants must follow these steps.

Step 1: With the form open, click on the **Submit Signed Documents to NRC** button. The cursor now changes to a black and white color wheel as the files are prepared and the Internet connection is attempted.

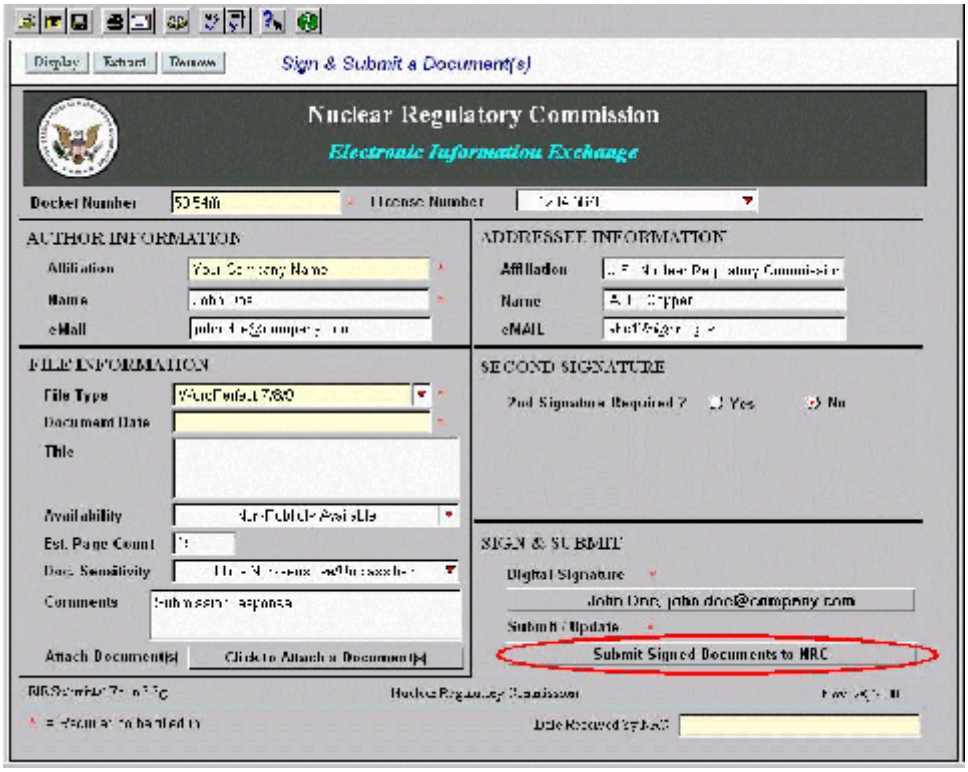

Figure 3-17: Submit Signed Documents to NRC

Step 2: Once the connection is established, the "Querying Browser" window appears and displays the progress of the file transmission.

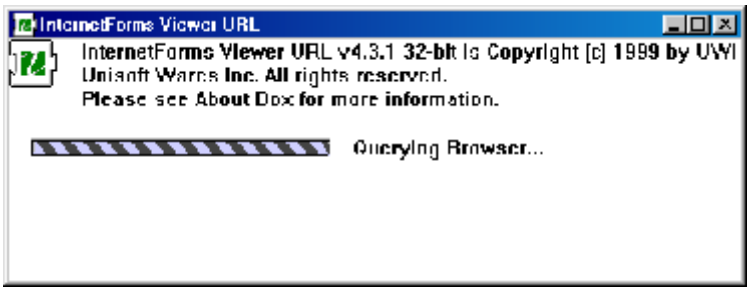

Figure 3-18: Querying Browser

Step 3: Once the form is successfully submitted, the browser flashes a window that states "Your Form Has Been Submitted."

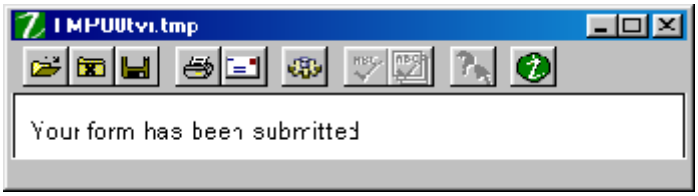

Figure 3-19: Successful Form Submittal Message

Step 4: Once the form has been submitted, close the form by clicking on the Close Form icon on the form toolbar. This returns you to the Submit/Retrieve Documents page.

Figure 3-20: Close form

Step 5: Exit the Submit/Retrieve Documents page and the browser by selecting **File** from the browser menu bar and click on **Exit** on the drop down menu.

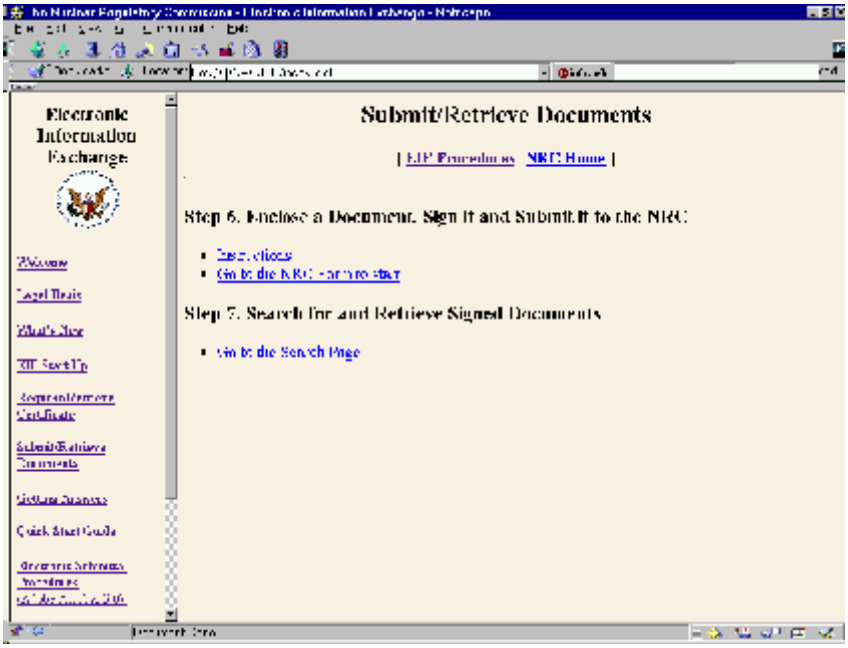

Figure 3-21: Exit Submit/Retrieve Documents Page

3.7 How to Remove Documents

During the process of enclosing documents, a situation may arise wherein a document is enclosed in error. In such situations, the erroneously enclosed document may be removed. The process for removing a document is outlined below.

Step 1: With the form open, click on the **Remove** button. This opens the Enclosures dialog box for removing documents.

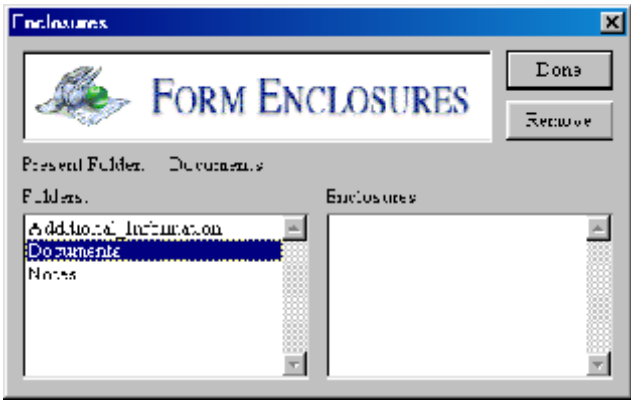

Figure 3-22: Remove Documents Dialog

Step 2: Highlight the Documents folder on the left side of the dialog box containing the document to be removed. The document(s) within the folder are displayed on the right side of the dialog box.

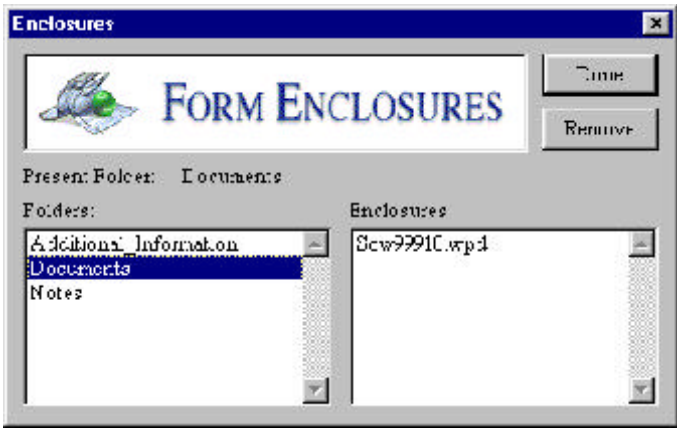

Figure 3-23: Document to be Removed

Step 3: Highlight the document to be removed and click on the **Remove** button. This produces a Remove Enclosure prompt.

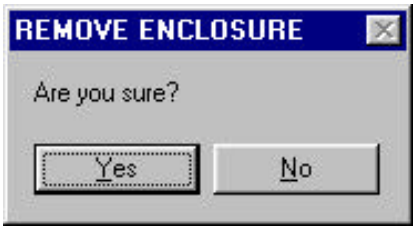

Figure 3-24: Remove Enclosure Prompt

Step 4: Click on the **Yes** button to remove the document.

4.0 HOW TO RETRIEVE DOCUMENTS

4.1 Introduction

When a form is submitted to the NRC external server, it is automatically date/time stamped at the time of receipt by the external server. This date/time stamp is intended to serve as the official date and time of receipt for both the NRC and it's customers. Intended recipients should receive an e-mail message providing notification of the submission and information necessary for it's retrieval such as; the author's name, author affiliation, document date, and docket number. Upon notification, recipients may access the external server and retrieve their documents. The steps involved in this process are as follows:

4.2 How to Search for Documents

Step 1: Open the Internet browser.

Step 2: Access the NRC EIE Startup page at http://www.nrc.gov/NRC/EIE/index.html. Once connected, click on the Submit/Retrieve Documents hyperlink. The Submit/Retrieve Documents page appears.

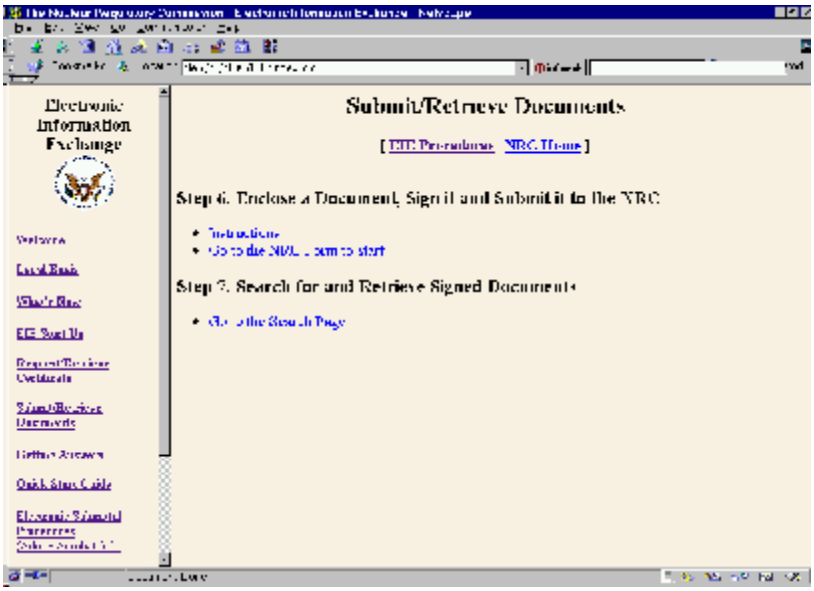

Figure 4-1: Submit/Retrieve Documents Page

Step 3: Click on the link, **Go to the Search Page**. The "Select a Certificate window appears.

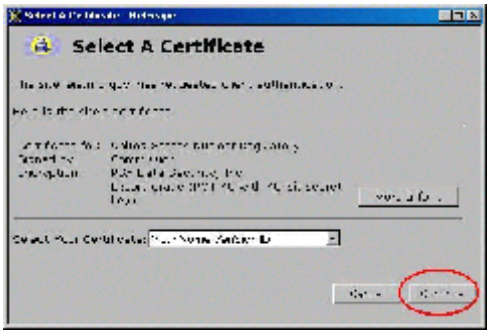

Figure 4-2: Select a Certificate

Select your NRC issued certificate and click on the **Continue** button. The Password Entry dialog appears.

Figure 4-3: Netscape Password Dialog Box

Step 3: Enter your password for the Certificate Database and click on **OK**. You will be prompted to re-enter it for confirmation, click on the **OK** button. A Security Information window appears, click on **Continue**.

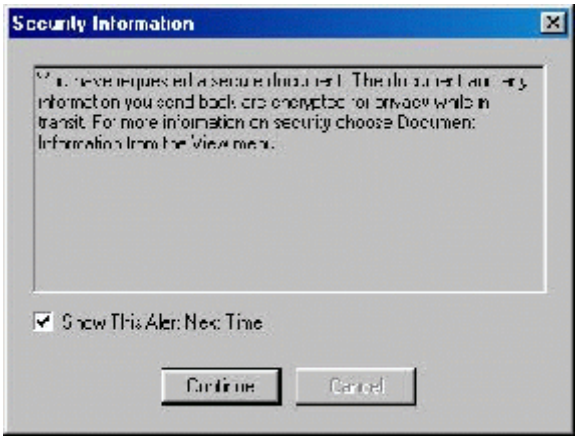

Figure 4-4: Security Information Window

Step 4: The Security Warning window now appears. Click on **OK** to continue.

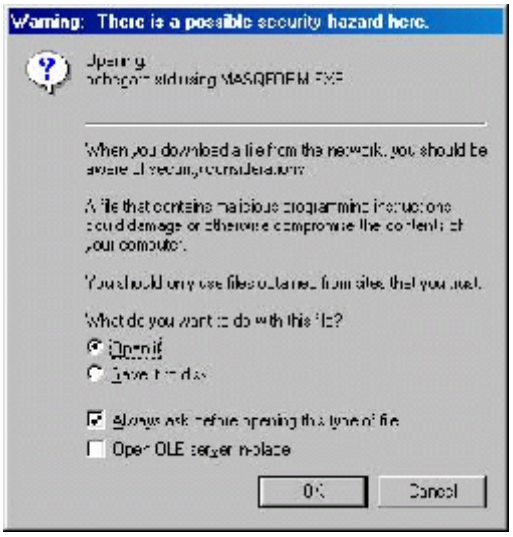

Figure 4-5: Security Warning Window

This produces the Search Form window.

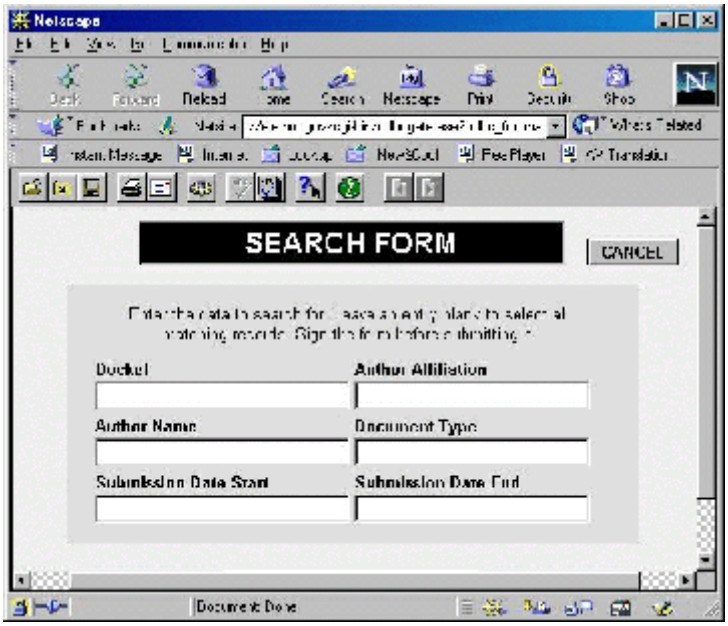

Figure 4-6: Search Form Dialog Window

Step 4: Enter search criteria.

The search criteria is used to search for the particular document sent to you. The search form allows searches to be performed on up to seven fields. Because search results provide matching records not only for the fields with information entered but also

for the fields left blank, it is recommended that all available information be entered. The applicable search fields include Docket, Author Name, Author Affiliation, Recipient, Document Type, Submission Date Start, and Submission Date End.

Step 5: Once the search criteria has been entered, click on the **Sign Form And Search** button. The Digital Signature Viewer appears.

Figure 4-7: Digital Signature Viewer

Step 6: Click on the **Sign** button. This initiates a check for your Digital ID.

Figure 4-8: Netscape Password Dialog Box

Step 7: Netscape users are asked for their password for the Certificate Database.

Once a valid Digital ID is found, the Digital Signature Viewer appears with the Digital ID signaturing information.

Figure 4-9: Digital ID Signaturing Information

Click on the **OK** button. This action signs the Search Form.

The Search Form appears as signed and a message stating this is returned. At the same time, the **Sign Form And Search** button is transformed to **Form Signed, Searching...** .

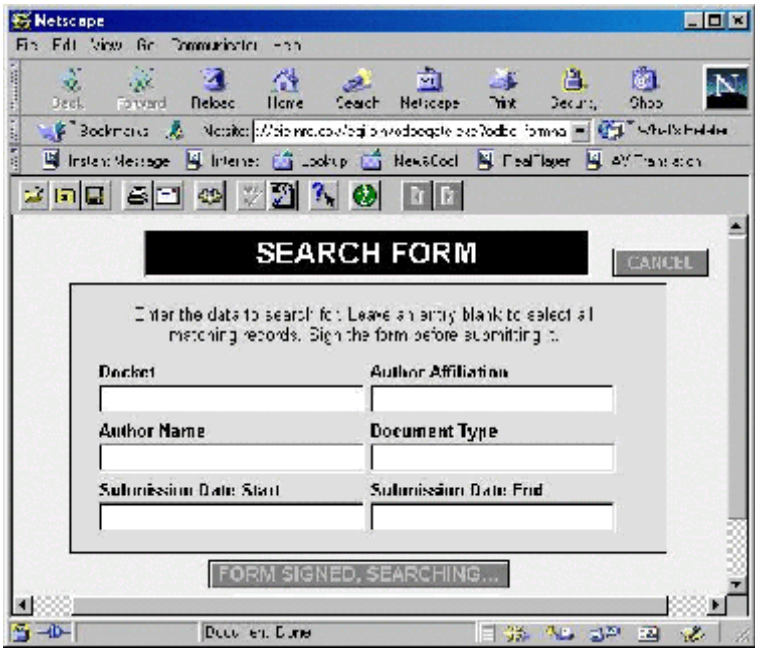

Figure 4-10: Signed Search Form

When the search is completed, the search results are returned listing the matching form or forms.

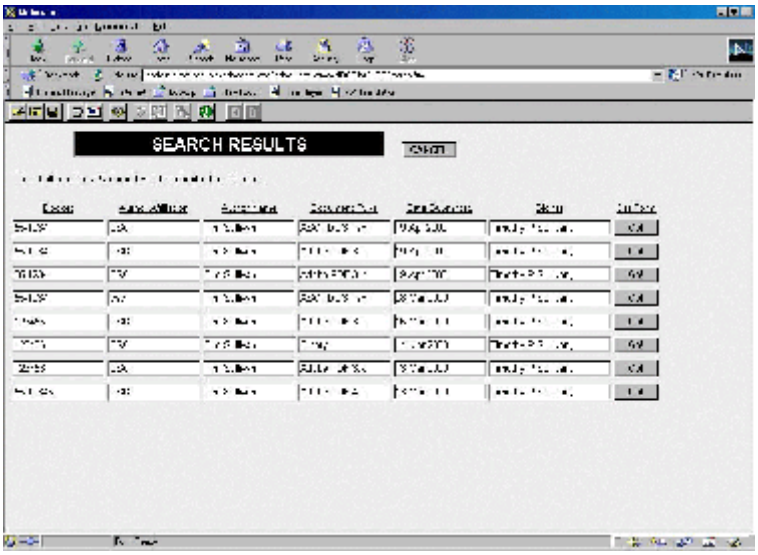

Figure 4-11: Search Results Dialog Window

The search results are returned in order of the date submitted and docket number. Once the list is provided, the form is ready to be retrieved. Locate the form to be retrieved and click on the **GO!** button on the right side of the listing. The submitted form is retrieved and displayed.

4.3 Authenticating the Form and Validating the Signature

Once the search for the appropriate form is complete and the form sought is digitally signed, the authentication and validation processes must be followed as outlined below.

Step 1: Once the form appears, click on the button displaying the sender's name and e-mail address to validate the signature and authenticate the form.

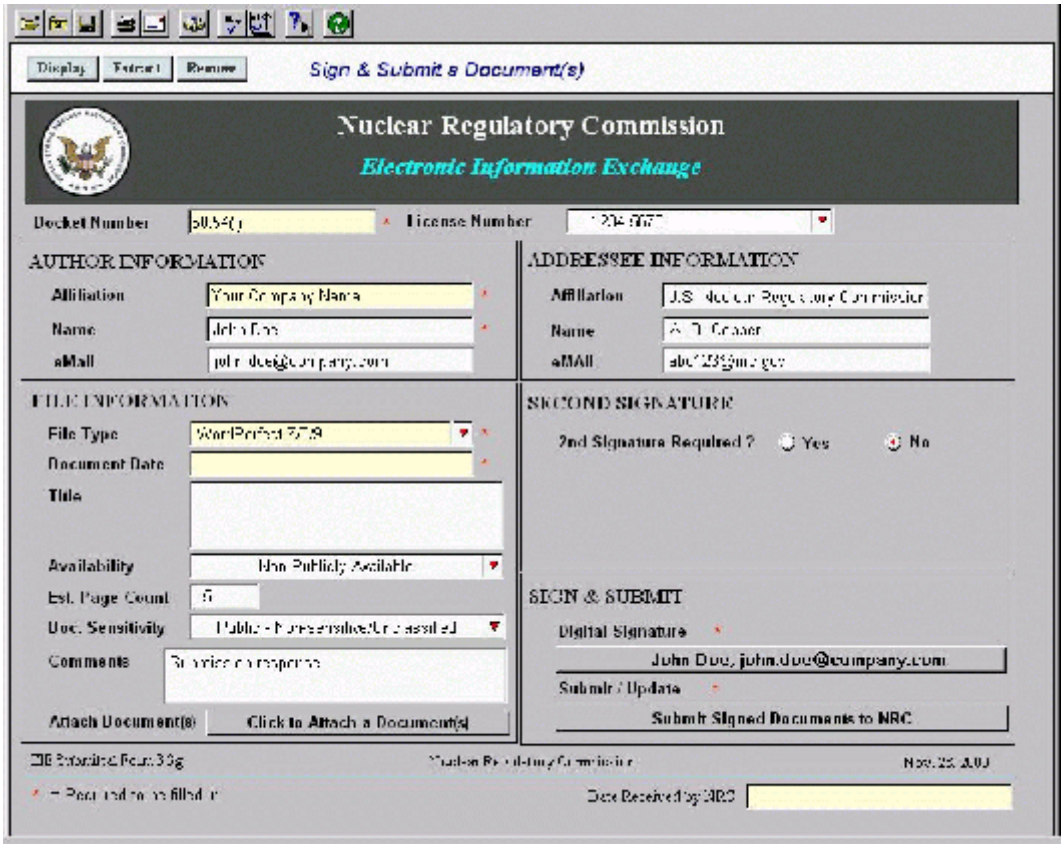

Figure 4-12: Signed NRC EIE Form

The Digital Signature Viewer appears.

Figure 4-13: Digital Signature Viewer – Signature is Valid

If the form has not been altered, the viewer appears with a message stating that the "Signature Is Valid" thus validating the signature and authenticating the form. The window also displays information about the signer.

Figure 4-14: Digital Signature Viewer – Signature is Valid

Step 3: After validating the signature, click on the **OK** button to return to the form. You may then proceed to retrieve the enclosed documentary material.

However, if the form has been altered, an error message appears stating that the **"form has been tampered with (form does not match signature hash value)."**

Figure 4-15: Altered Form Error Message

If the form has been altered, click on the **OK** button to return to the form and promptly notify the LRA at pgn1@nrc.gov. The LRA will notify the sender of the alteration and request re-submission.

4.4 Document Access and Retrieval

After locating the form and validating the signature, participants can proceed to access, view, and retrieve any documents enclosed in the form. Enclosed documentary material can be viewed using the form's display function or retrieved using the form's extract function. The steps involved in performing each function are listed below.

Displaying Documents

Step 1: With the form open, click on the **Display** button on the form. The "Enclosures" dialog window appears.

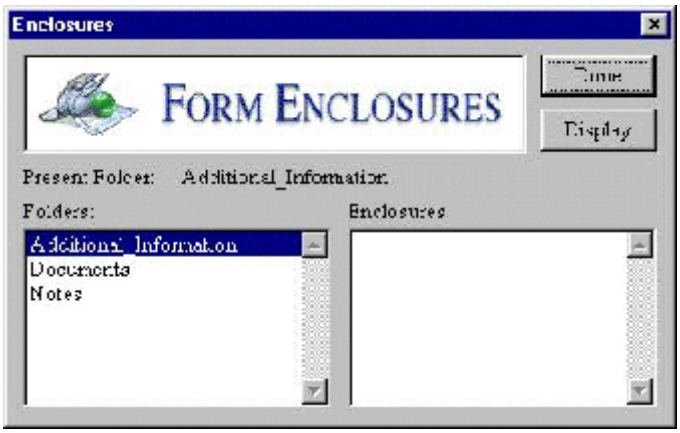

Figure 4-16: Enclosures Dialog Window

Step 2: Select the folder containing the documents to be viewed by clicking the folder name in the folder window. The enclosed document file names now appear on the right side of the dialog box in the "Enclosures" window.

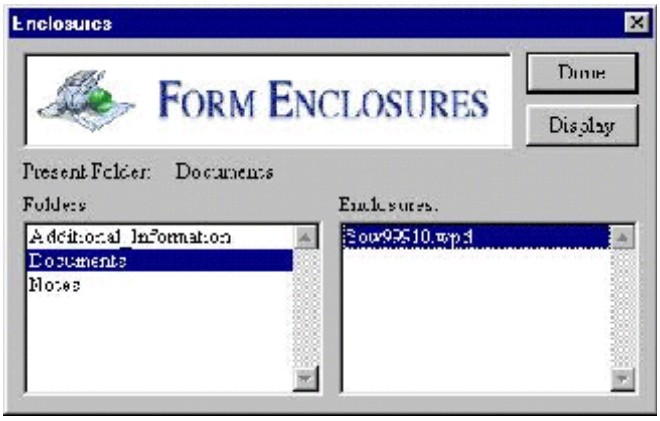

Figure 4-17: Display Enclosures Window

Step 3: Highlight the document file name and click on the **Display** button. This invokes the browser and produces a Security Warning Dialog.

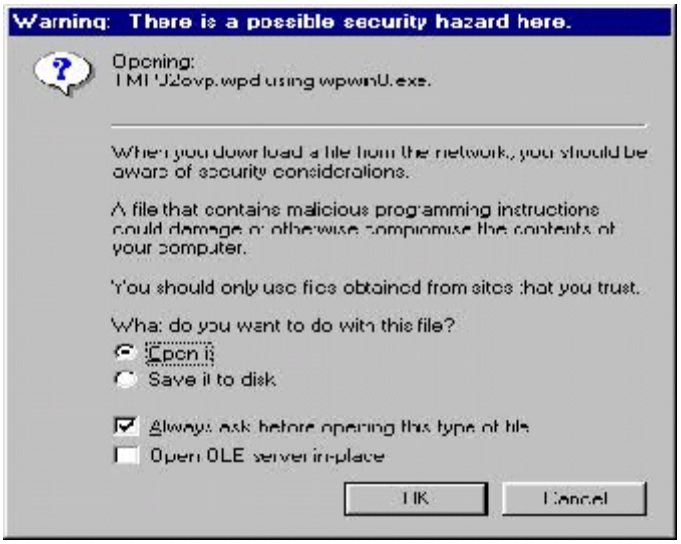

Figure 4-18: Warning Dialog Window

Step 4: Click on the **OK** button to open the document or check the **Save to Disk** radio button and click **OK** to download the document to your workstation or local network drive.

Retrieving Documents

In order to retrieve documents from the external server directly to your workstation or local network, participants can use the form's extract function. The process to extract a document is the reverse of the process to enclose a document. The steps involved in the extraction process are as follows.

Step 1: With the form open, click on the **Extract** button. The "Enclosures" dialog box appears.

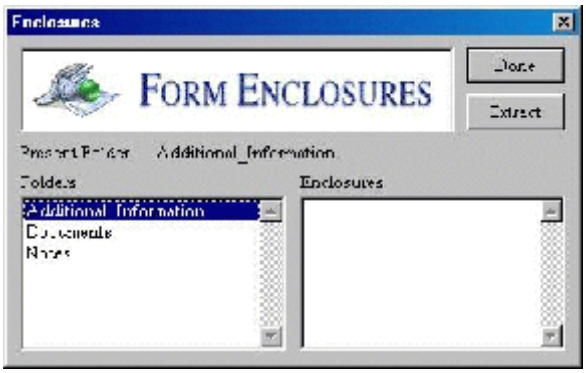

Figure 4-19: Enclosures Dialog Window to Extract Documents

Step 2: Click on the folder name containing the document(s) to be extracted in the folder window on the left side of the dialog window. The enclosed document file name(s) appears in the "enclosures" window on the right side of the dialog box.

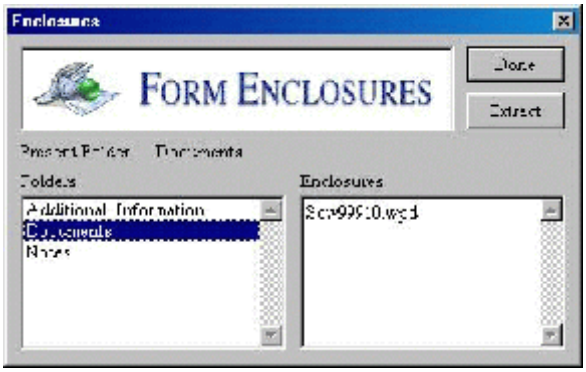

Figure 4-20: Enclosure Dialog with Document File Displayed

Step 3: Highlight the document file name and click on the **Extract** button.

The Extract File window is now open.

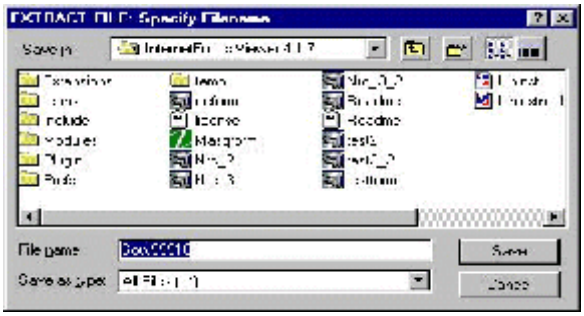

Figure 4-21: Extract File Window

Step 4: Navigate to the local or network drive and folder or subdirectory where you intend to store the document file. Once there, click the **Save** button to extract the document from the form and to place it in the chosen folder or subdirectory. You are then returned to the Enclosure dialog. If there are multiple documents to extract, repeat this process until all have been extracted.

Step 5: When all documents have been extracted, click on the **Done** button on the Enclosure dialog box. This returns you to the form.

4.5 Deleting and Saving Forms

Participants should not attempt to delete or remove forms from the external server since forms may be intended for multiple recipients. The responsibility for file maintenance resides with the NRC EIE system administrator. If a form or form package is uploaded to the external server by mistake, participants should notify the LRA at pgn1@nrc.gov. If a participant wishes to retain a copy of the form, follow the steps listed below.

Step 1: Click on the **Save** icon on the form's menu bar.

Figure 4-22: Save form

This opens the Save Form window.

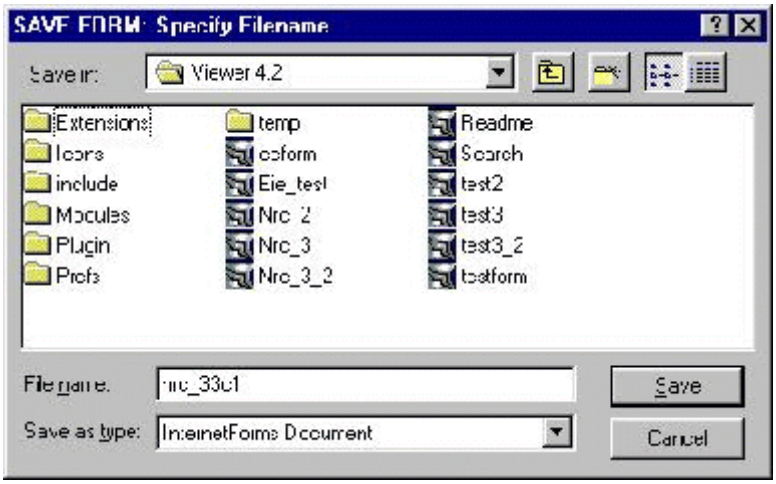

Figure 4-23: Save Form Window

Step 2: With the Save Form window open, specify a file name.

Step 3: Then, navigate to the appropriate drive, folder, or directory in which to save the file.

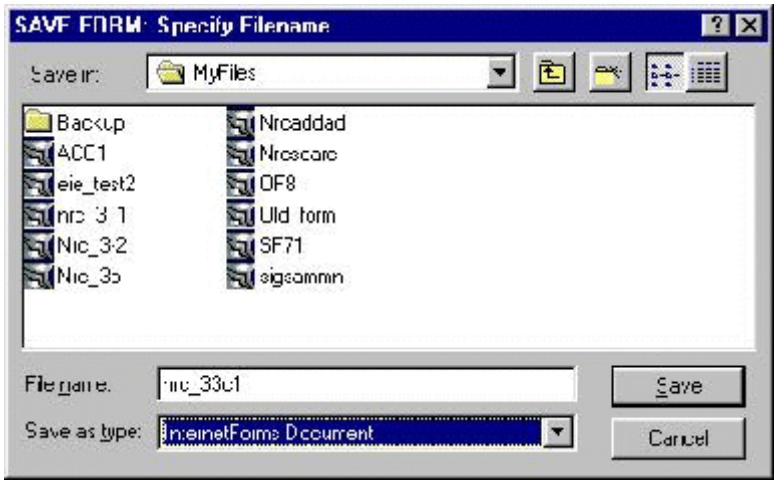

Figure 4-24: Save Form Window

Step 4: Click on the **Save** button. All forms are saved with the file extension ".xfd."

5.0 DIGITAL ID MANAGEMENT

5.1 Introduction

Once your Digital ID and key files have been deleted, damaged or overwritten, there is no way to reactivate your Digital ID. A hard drive crash usually deletes all key pair and Digital ID files in your computer. If this happens and you have no backup copy, you must revoke your digital certificate and enroll for a new one.

If your computer is stolen, it is unlikely that the thief will be able to use your digital certificate to impersonate you because your key files are protected with a password. In Microsoft Internet Explorer, your key files are protected by your Windows password, and in Netscape they are protected by your Navigator or Communicator password. However, if this happens, immediately revoke your Digital ID and enroll for a new one.

The following sections provide instructions and frequently asked questions (FAQs) for managing your Digital ID.

5.2 How to Search for a Digital ID

Go to the NRC EIE Home page at http://www.nrc.gov/NRC/EIE/index.html and click on the hyperlink Request/Retrieve Certificate.

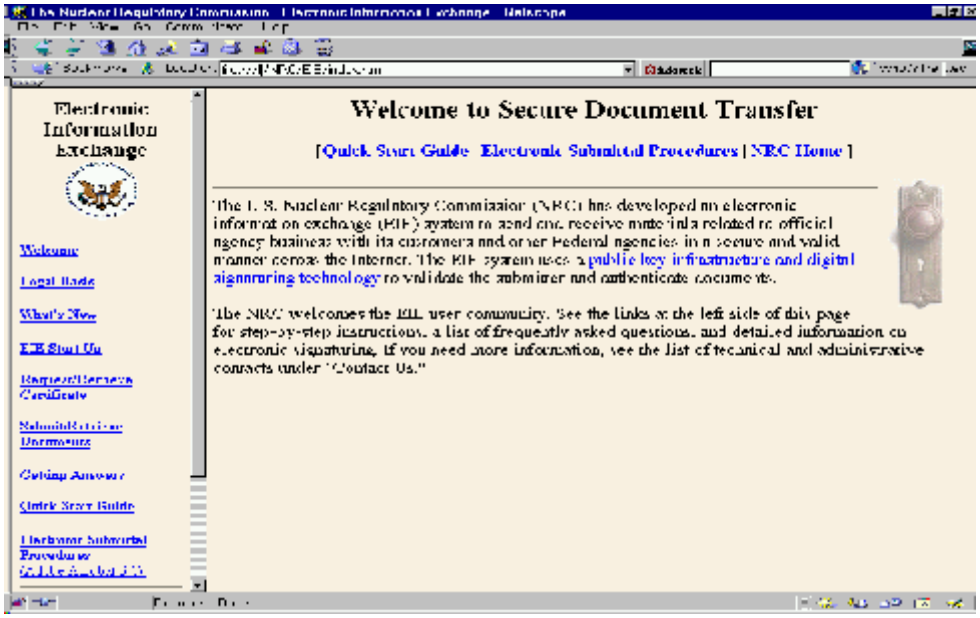

Figure 5-1: NRC EIE Home Page

The Request/Retrieve Certificate page appears. Under Step 3, click on the Go to the VeriSign/NRC Page hyperlink.

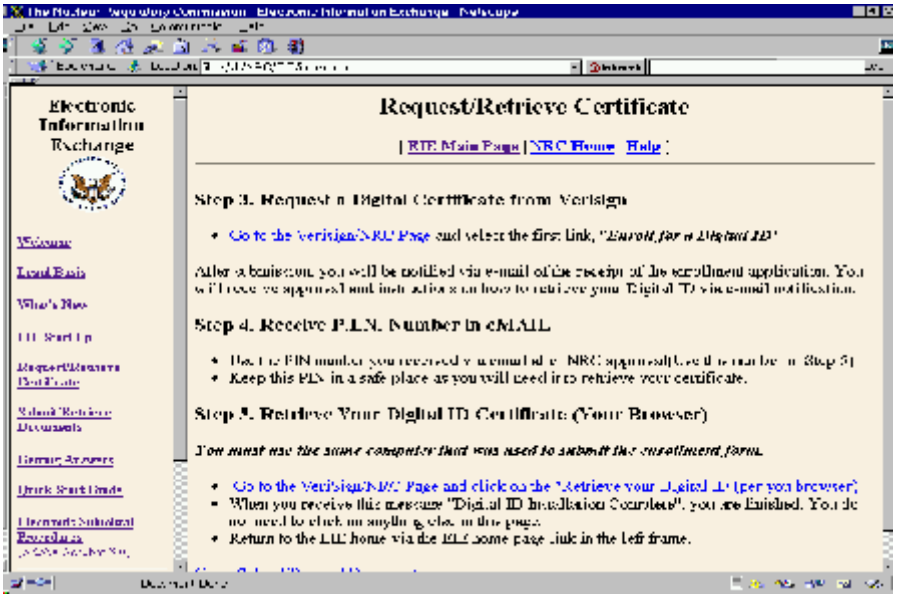

Figure 5-2: Request/Retrieve Certificate Page

The VeriSign Onsite End-User Services page now appears.

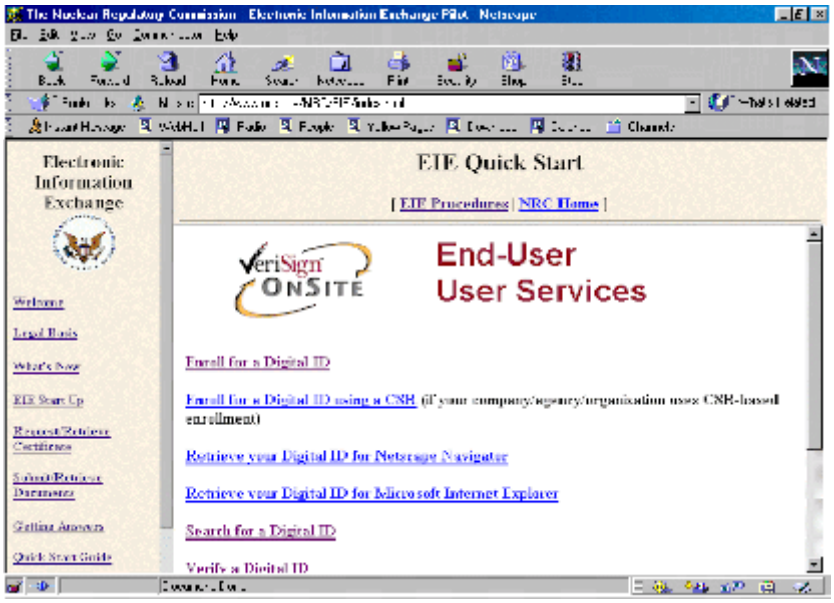

Figure 5-3: VeriSign Onsite End-User User Services

Step 1: Click on the **Search for a Digital ID** or **Verify a Digital ID** hyperlink.

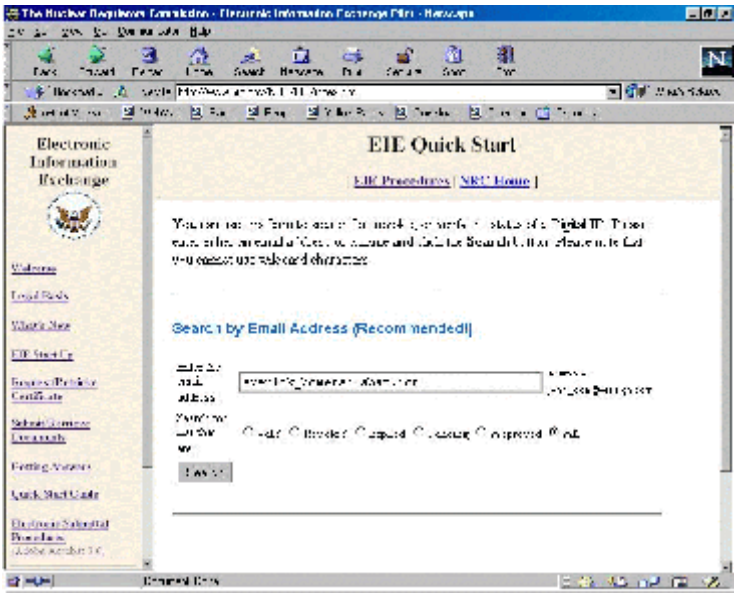

Figure 5-4: Digital ID Search

This will allow you to search the online directory of Digital IDs by entering an E-mail address or name. A successful search will return all matching certificates that show Digital ID status (valid, revoked, expired, pending, or approved) and the validity period.

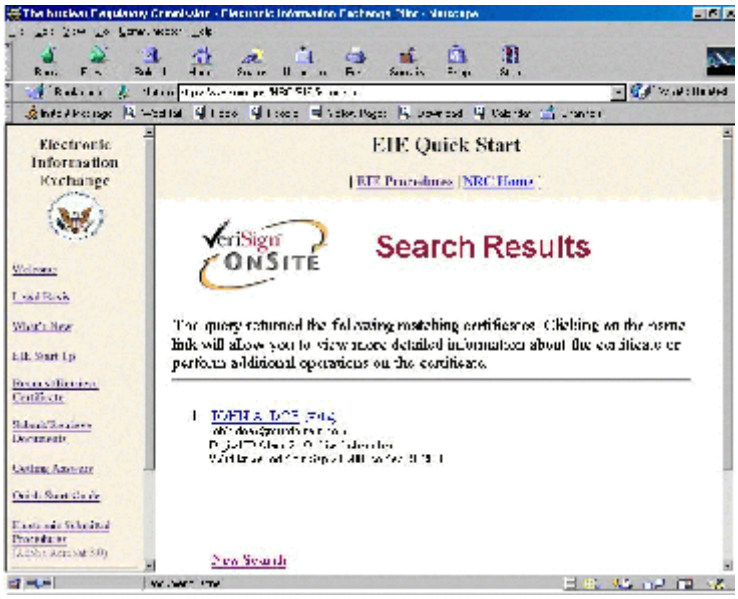

Figure 5-5: Digital ID Search Results

Use the search capability to monitor the validity or exact date that your Digital ID expires.

5.3 How to Save a Backup Copy of Your Digital ID

A backup copy of your Digital ID should be saved in case your hard drive crashes or your Digital ID files are accidentally deleted. By storing a backup copy of your Digital ID on a floppy disk in a secure place, you will always be able to re-install your Digital ID. If you lose your Digital ID and it is not backed-up, then you will lose any messages that have been encrypted for you. To create a backup copy of your Digital ID, follow the steps outlined below.

Netscape Users Only

Step 1: Click on the Security icon (the one that looks like a padlock) from the main toolbar.

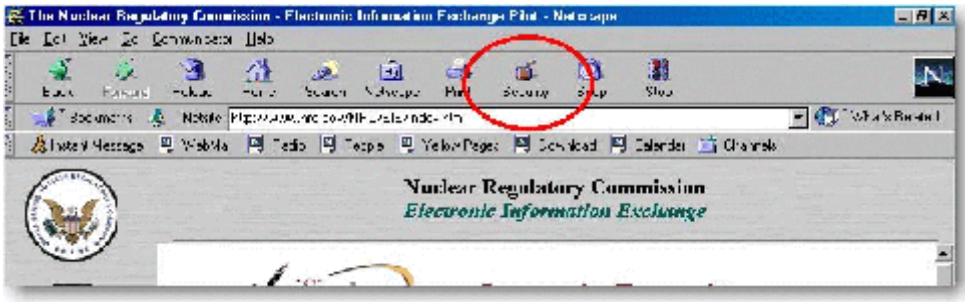

Figure 5-6: Netscape Toolbar

Step 2: Click on **Yours** under **Certificates** from the menu on the left.

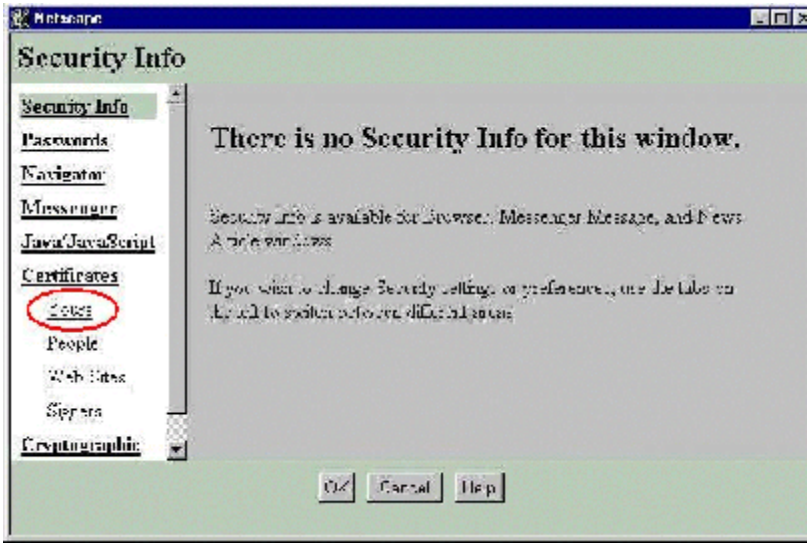

Figure 5-7: Security Info Window

Step 3: Highlight the Digital ID you want to save, then click on the **Export** button.

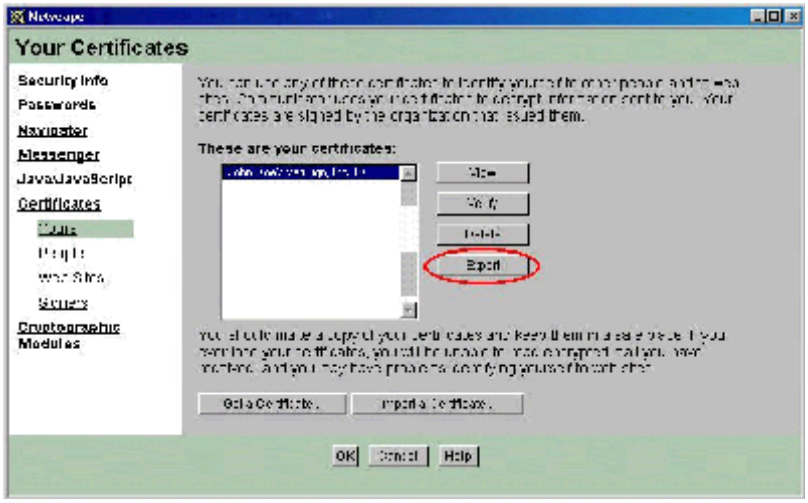

Figure 5-8: Select Certificate to Export

Step 4: Choose a transport password, which you will be required to present when importing (re-opening) your Digital ID, then click on **OK**.

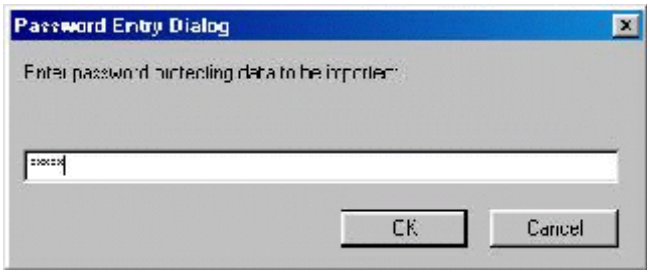

Figure 5-9: Password Entry Dialog

Step 5: Select a location (such as your floppy disk) and file name in which to save your Digital ID, then click on **Save**.

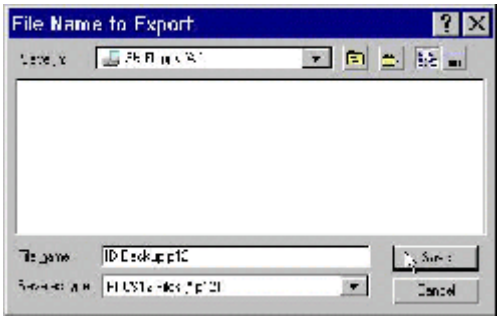

Figure 5-10: File Export

Step 6: Save your floppy disk and your transport password in a safe location.

Microsoft Internet Explorer Users Only

Step 1: From the **View** menu of Explorer, choose "Internet Options ..."

Figure 5-11: Internet Explorer Drop Down Menu

Step 2: Select the **Content** tab.

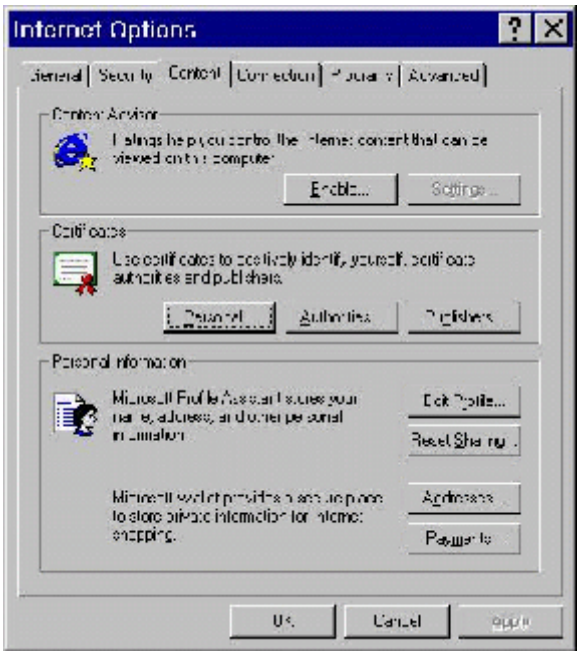

Figure 5-12: Internet Options Tabs

Step 3: Select **Personal** from the Certificates list.

Step 4: Highlight the Digital ID you wish to save, then click on the **Export** button.

Figure 5-13: Select Certificate

Step 5: Choose a password and a file name for your Digital ID. This new password protects this specific copy of your Digital ID -- you will be required to present it when you want to import or open this copy of your digital certificate. Be sure to include a disk and folder location in the file name, such as a: if you want to save to a floppy disk. Click on **OK**.

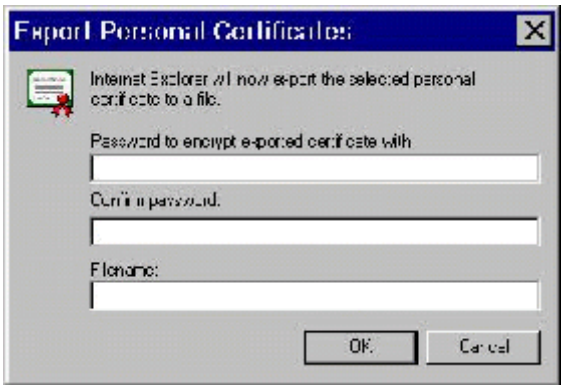

Figure 5-14: Choose Password to Export Certificate

Step 6: If prompted, enter the security password you have always used to protect your Digital ID. You may be prompted to enter this password multiple times before it takes.

Step 7: Save your floppy disk and your transport password in a safe location.

5.4 How to Transfer Your Digital ID to Another Computer

The first step for transporting your Digital ID is to save ("export") it from the hard drive of the computer where it is currently held onto a floppy disk or other transport medium (see

Section above). When your Digital ID has been successfully exported, you can then import it into the new location.

Netscape Users Only

To import your Digital ID into Netscape:

Step 1: Click on the security icon (the one that looks like a padlock) from the main toolbar.

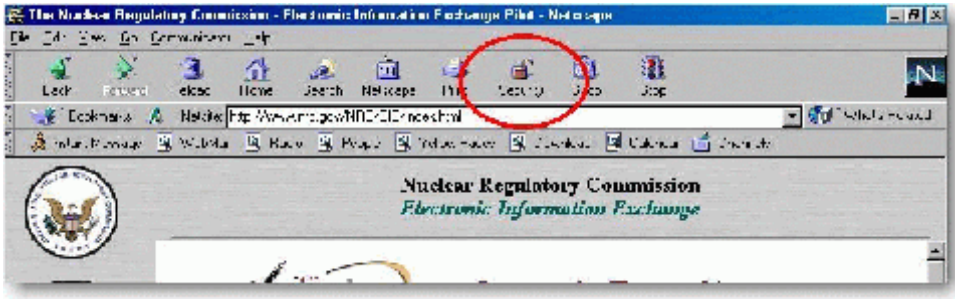

Figure 5-15: Netscape Toolbar

Step 2: Click on **Yours** under **Certificates** from the menu on the left.

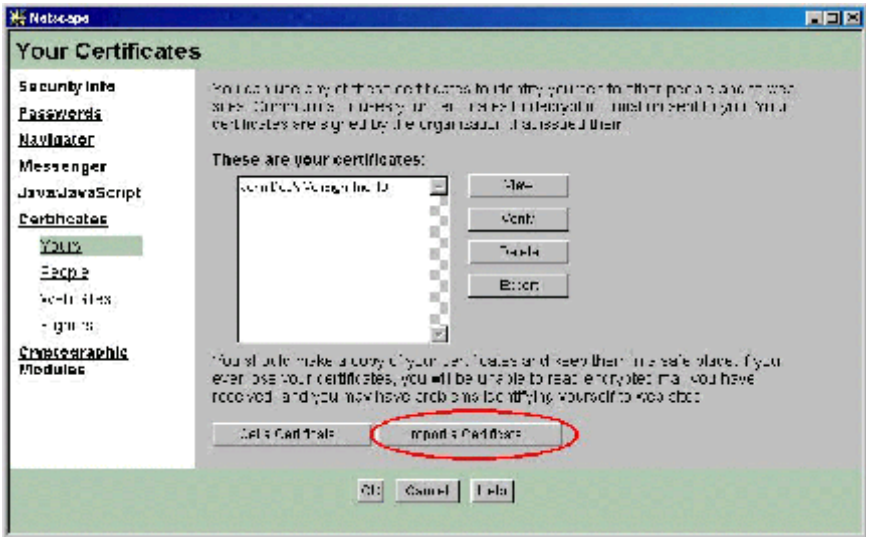

Figure 5-16: Select Certificate to Export

Step 3: Click on the **Import Certificate** button located at the bottom of the page.

Step 4: If prompted, enter the password used to protect your Digital ID (this is NOT the transport password, but the security password you use each time you present your Digital ID). You may be prompted to enter this password multiple times before it takes.

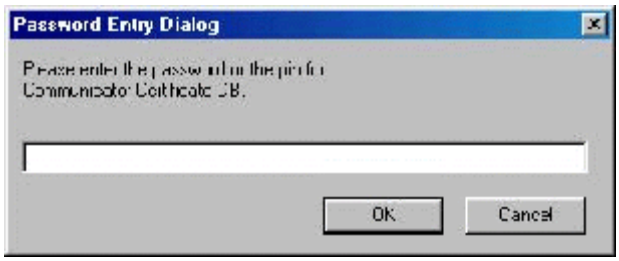

Figure 5-17: Password Entry Dialog

Step 5: Locate your Digital ID from the disk and folder in which it is saved (it should have a .pfx or .p12 extension). Once you have found it, highlight it and click on **Open**.

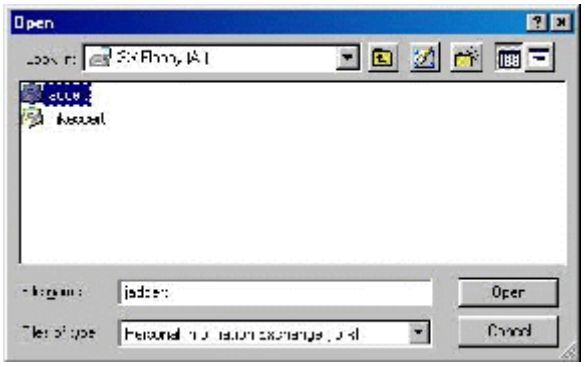

Figure 5-18: Locating Certificate

Step 6: Enter your transport password and click on OK. (If your Digital ID shows up as a long series of numbers or letters, it should still work correctly.)

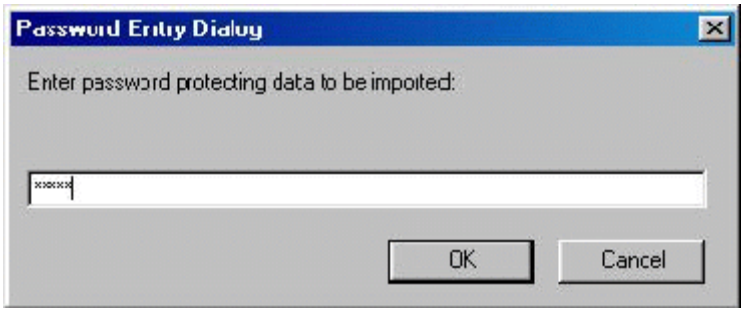

Figure 5-19: Password Entry Dialog

To remove your Digital ID and key files from the old computer:

Step 1: Click on the security icon from the main toolbar.

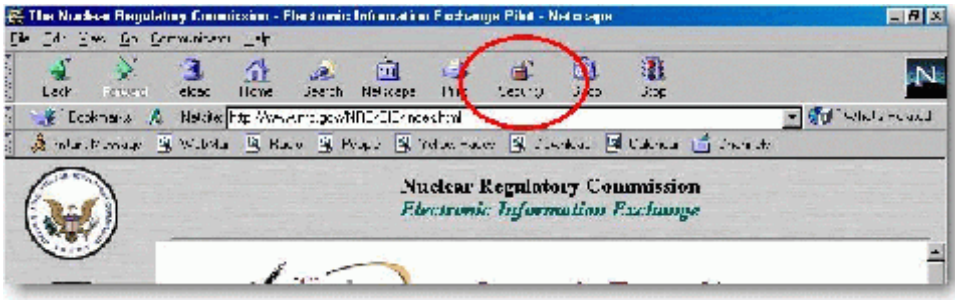

Figure 5-20: Netscape Toolbar

Step 2: Click on **Yours** under **Certificates** from the menu on the left.

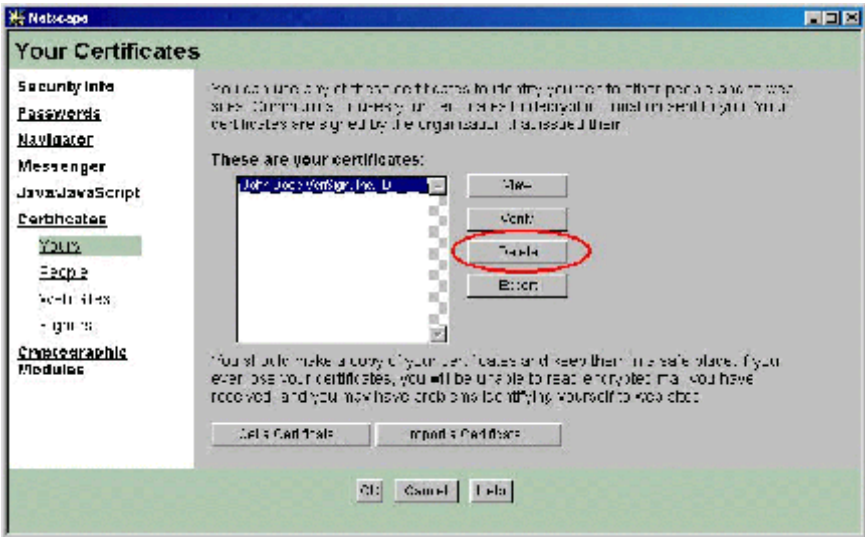

Figure 5-21: Select Certificate to Delete

Step 3: Select the Digital ID to be removed, then click on the **Delete** button.

Microsoft Internet Explorer Users Only

To import your Digital ID into Internet Explorer:

Step 1: From the Internet Explorer toolbar, select **View** and choose "Internet Options ..." from the drop down menu.

Figure 5-22: Internet Explorer Drop Down Menu

Step 2: Select the **Content** tab.

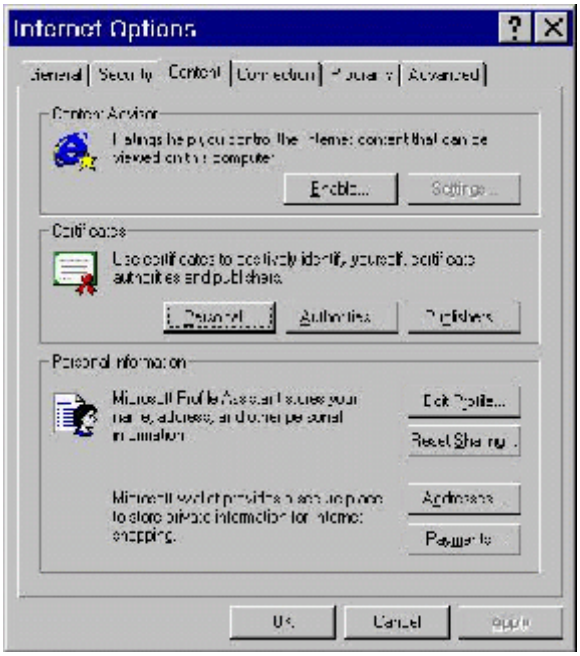

Figure 5-23: Internet Options Tabs

Step 3: Select **Personal** from the Certificates list. This opens the Certificate Manager.

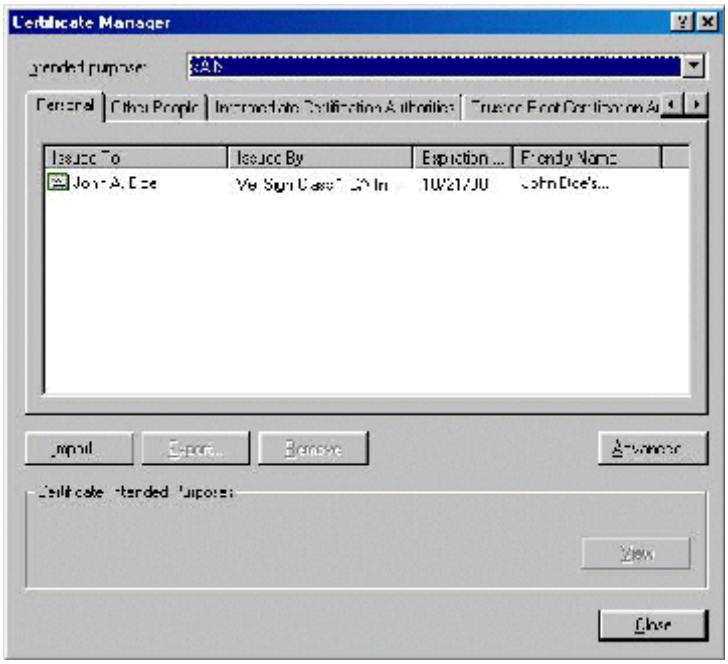

Figure 5-24: Certificate Manager

Step 4: Click on the **Import** button. This will invoke the Certificate Manager Wizard.

Figure 5-25: Certificate Manager Wizard

Step 5: Click on Next and then browse to locate your Digital ID from the disk or folder in which it is saved (it should have a .pfx or .p12 extension).

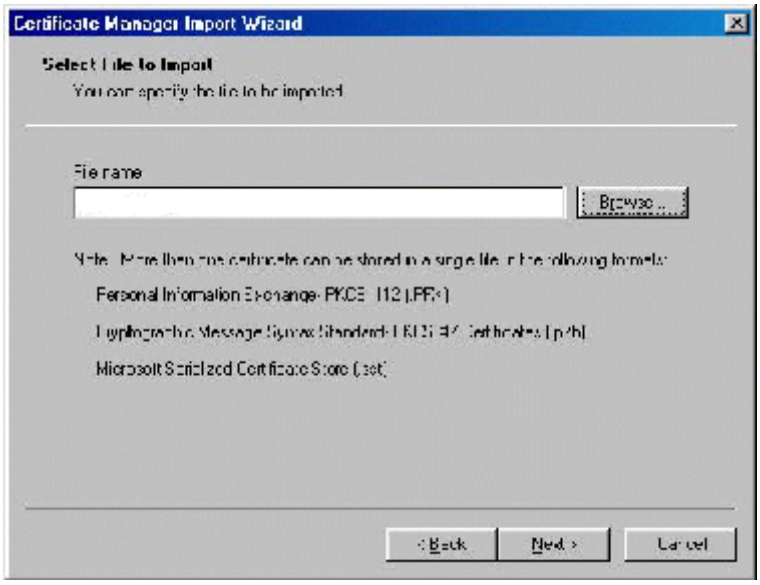

Figure 5-26: Certificate Manager Import Wizard

Once you have found it, highlight it and click on **Open**.

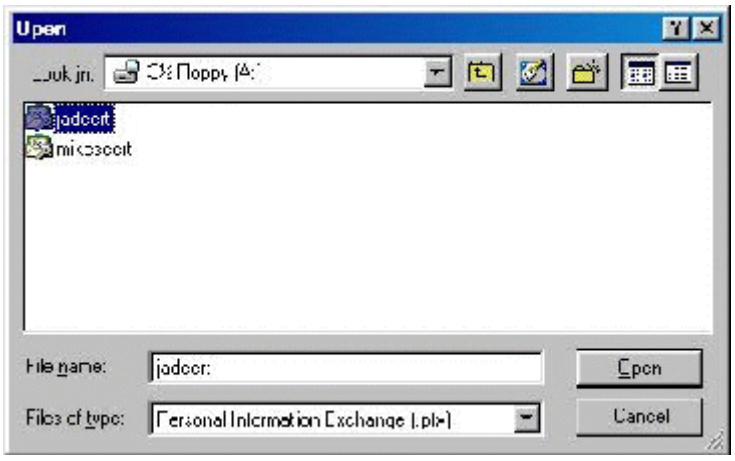

Figure 5-27: Locating Certificate

The certificate is inserted in the browse window of the Certificate Manager Wizard. Click on Next to proceed.

Step 6: When prompted, enter the import password used to protect your Digital ID (this is the same password used to export your Digital ID). You may be prompted to enter this password multiple times.

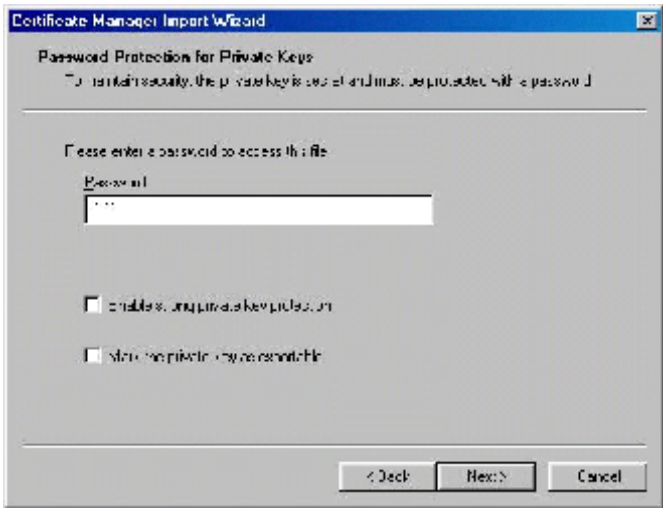

Figure 5-28: Password Dialog

Step 7: Enter your password and click **Next**. You will then be prompted to select the certificate store. This is set to a default of automatic. Simply click **Next** and then **Finish**.

To remove your Digital ID and key files from the old computer:

Step 1: From the Internet Explorer toolbar, select **View** and choose "Internet Options ..." from the drop down menu.

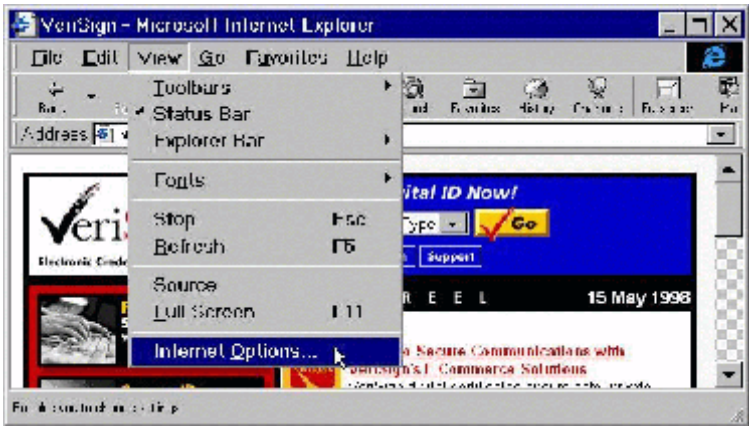

Figure 5-29: Internet Explorer Drop Down Menu

Step 2: Select the **Content** tab.

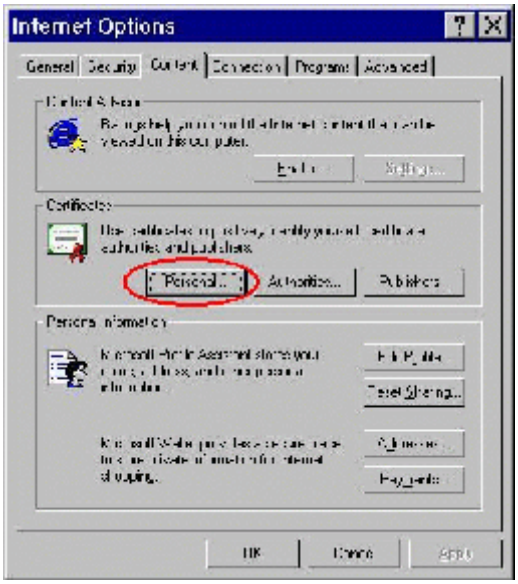

Figure 5-30: Internet Options Tabs

Step 3: In the Certificates section, click on the **Personal** button.

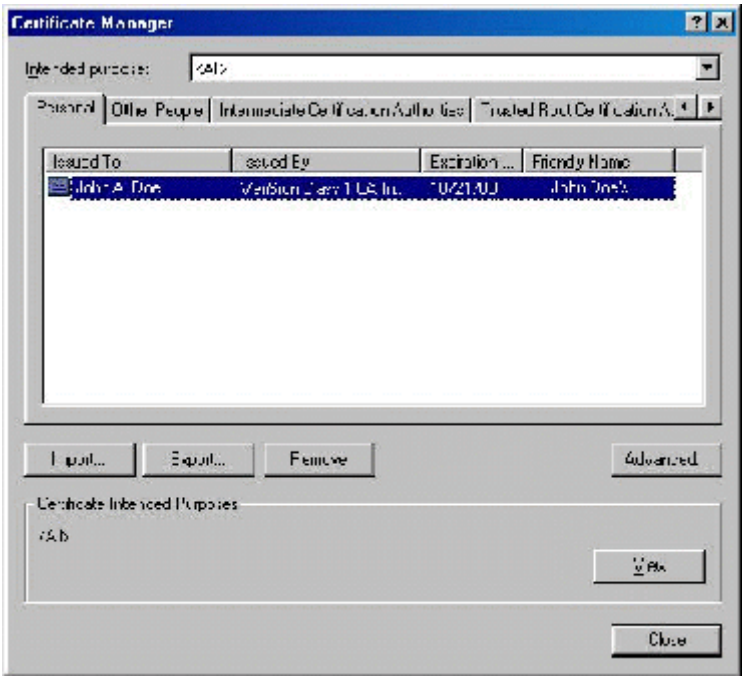

Figure 5-31: Personal Certificate in Certificate Manager

Step 4: Highlight the Digital ID to be removed, then click on the **Remove** button.

5.5 How to Renew Your Digital ID

A Digital ID is valid for one year from the time that it is installed. Approximately two to three weeks prior to the date of expiration, you will receive an e-mail notification of the pending expiration. Included in the e-mail is a hyperlink to the VeriSign Onsite Digital ID Center and a personal identification number (PIN) required for identification purposes. To renew you Digital ID, follow the steps outlined below.

Step 1: Access the VeriSign Onsite Digital ID Center using the following URL. https://onsite.verisign.com/services/ USNuclearRegulatoryCommissionADDOCIO/ digitalidCenter.htm. The Digital ID Center page is displayed.

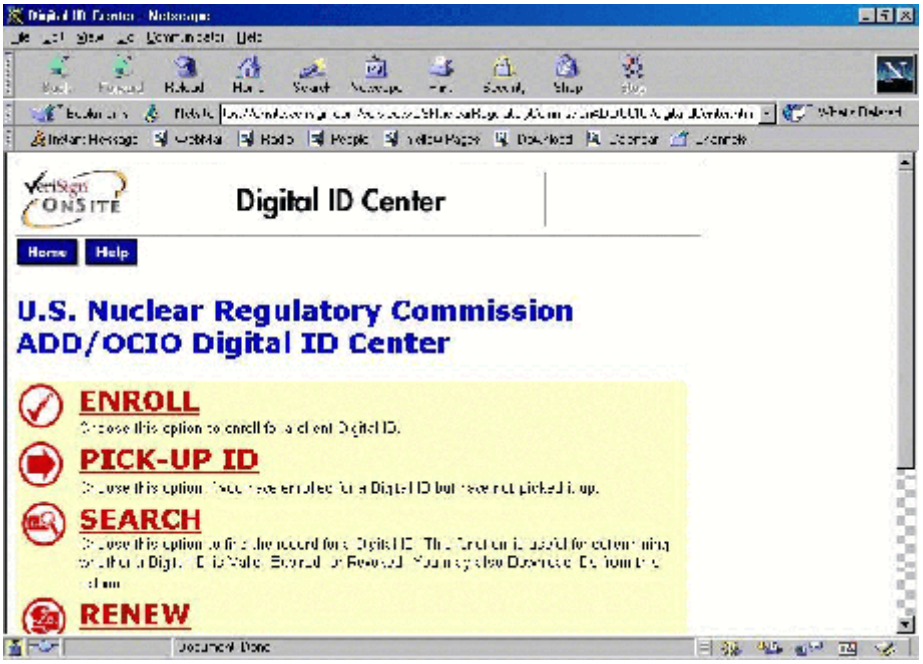

Figure 5-32: Digital ID Center

Step 2: Click on the Renew option. This will produce the Digital ID Renewal page.

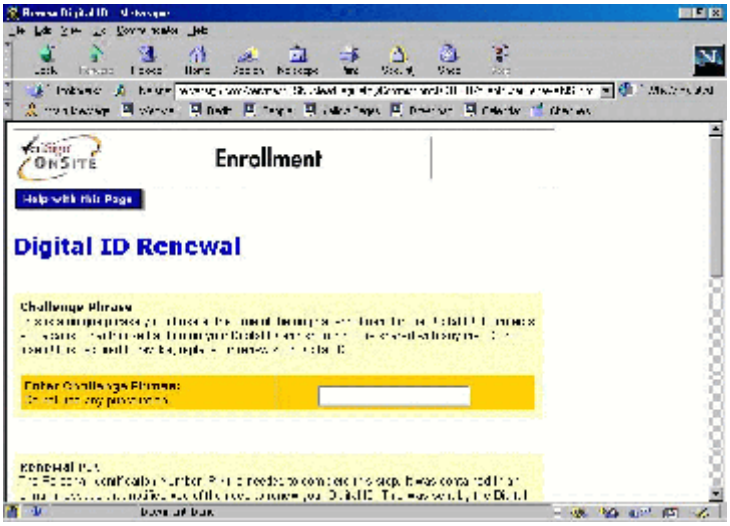

Figure 5-33: Digital ID Renewal

Step 3: In order to renew your Digital ID, you will need your Challenge Phrase, which you entered during enrollment. Enter your **Challenge Phrase**. If you do not remember the challenge phrase you will have to enroll for a new Digital ID.

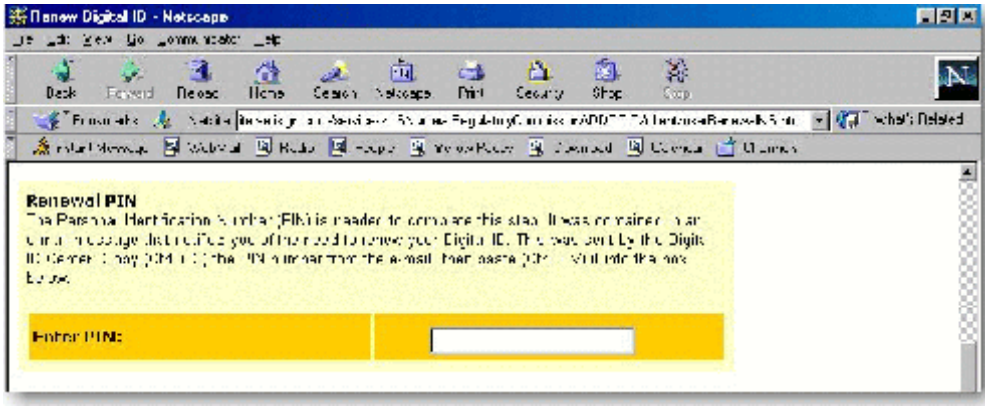

Figure 5-34: Renewal PIN Entry

Step 4: Enter the PIN number included in the Digital ID renewal e-mail.

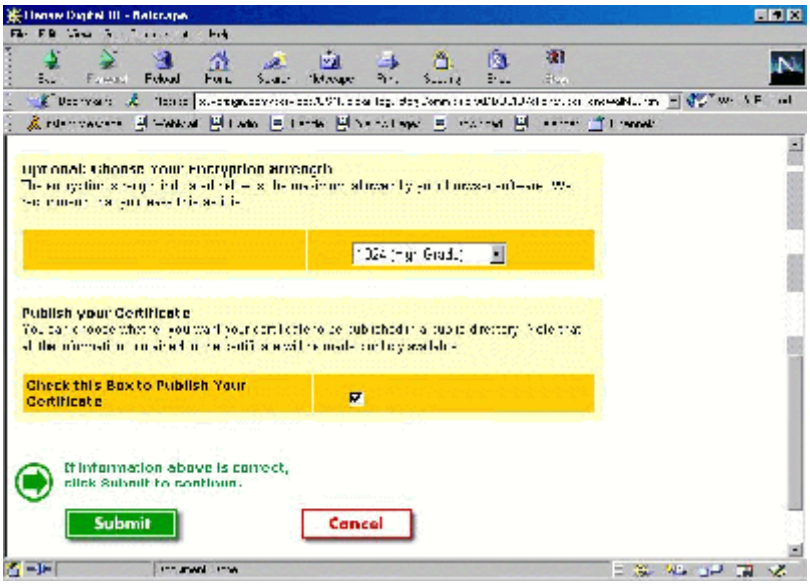

Figure 5-35: Completing Renewal

Step 5: Select the desired encryption strength and be sure that the "Publish your Certificate" box is checked. Then click on the **Submit** button to complete the process. Within 24 to 48 hours, you will receive e-mail notification with instructions on picking up and installing your renewed Digital ID. Follow the instructions as outlined in the e-mail and Section 2.5, Retrieving and Installing the Digital ID Certificate.

5.6 How to Revoke Your Digital ID

You need to revoke your Digital ID if its security has been compromised, or if you lost the ability to use it and want a replacement. For example, if somebody stole your computer with your private key file and you had not protected this file with a password, that person could read your encrypted messages and impersonate you on the Internet. You should revoke (cancel) your Digital ID so that VeriSign will no longer vouch for the holder of that Digital ID. Alternatively, if your hard drive crashed and you lost your private key file, you will be unable to use your digital certificate. In this case you should revoke the Digital ID so that you can get a new key pair and a replacement Digital ID.

To revoke your Digital ID, go to the NRC EIE Home page at: http://www.nrc.gov/NRC/EIE/index.html. Click on the hyperlink Request/Retrieve Certificate.

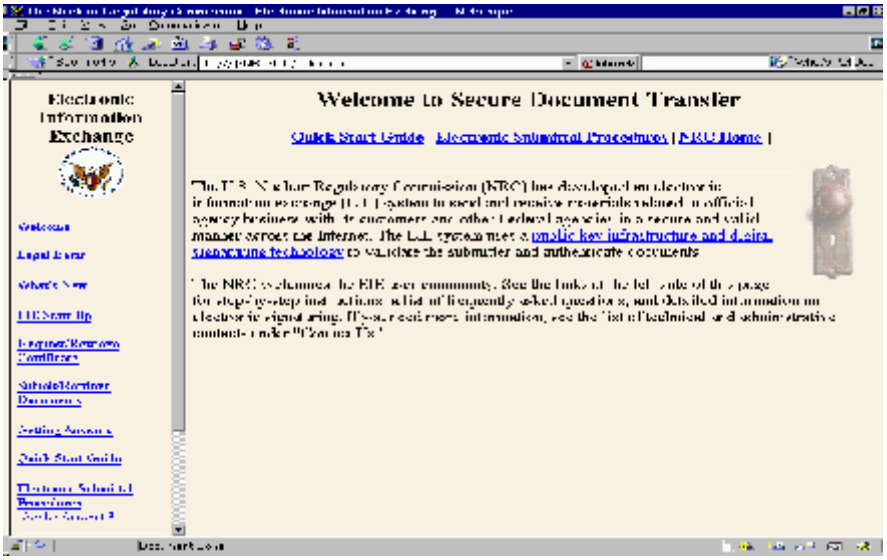

Figure 5-36: NRC EIE Home Page

This produces the Request/Retrieve Certificate page.

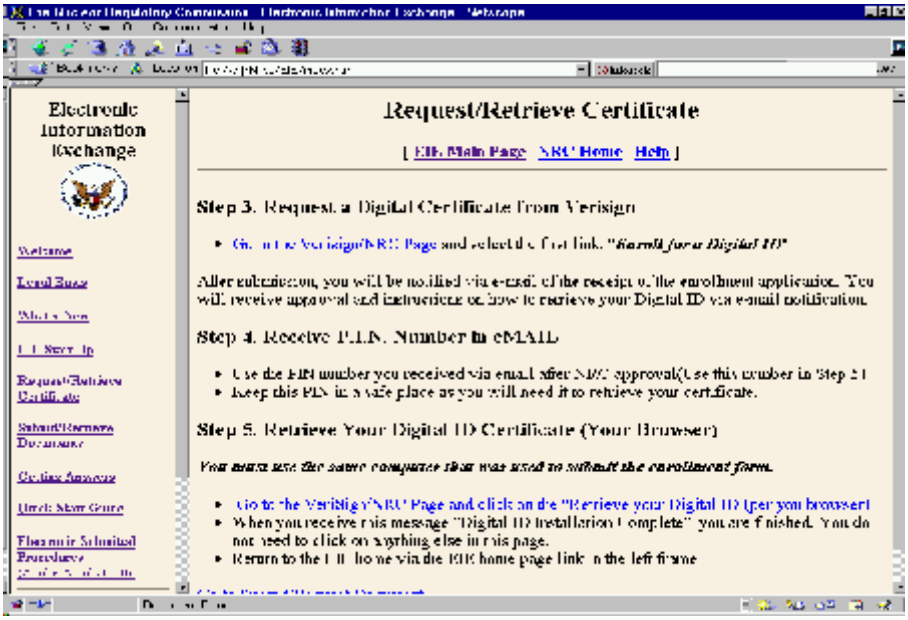

Figure 5-37: Request/Retrieve Certificate Page

From the Request/Retrieve Certificate page, click on the Go to VeriSign/NRC Page link under Step 3. This produces the VeriSign Onsite End-User Services page.

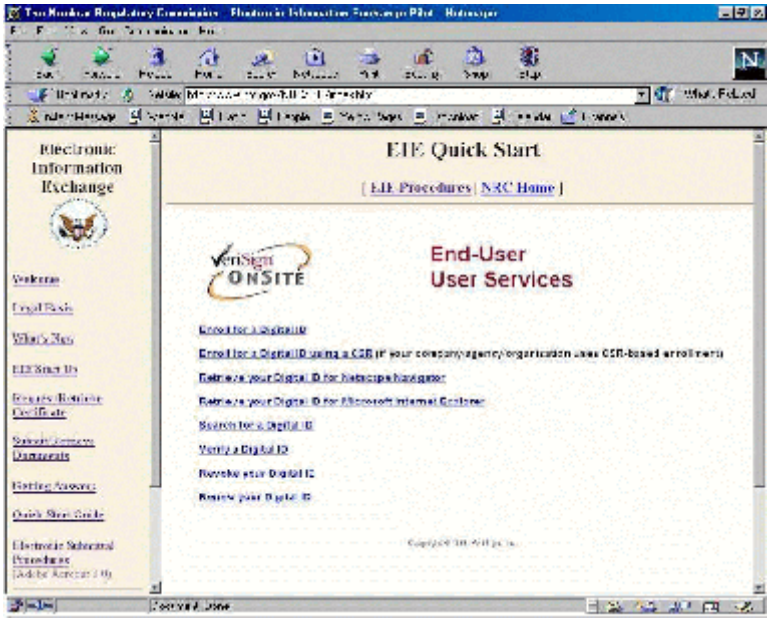

Figure 5-38: VeriSign Onsite End-User Services Page

Click on the **Revoke your Digital ID** button. You will need your challenge phrase, which you entered during enrollment.

Follow the steps below to revoke the Digital ID:

Step 1: Find your Digital ID (see How to Search section above).

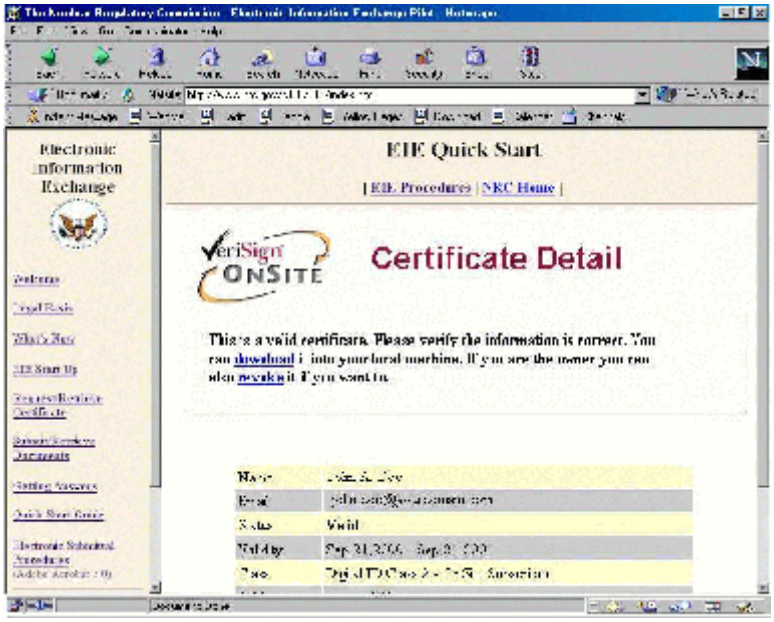

Figure 5-39: Certificate Detail

Step 2: Verify that it is the correct Digital ID.

Step 3: Enter your challenge phrase and specify a reason for revocation. The pull-down box shows the most common revocation reasons. Select a reason.

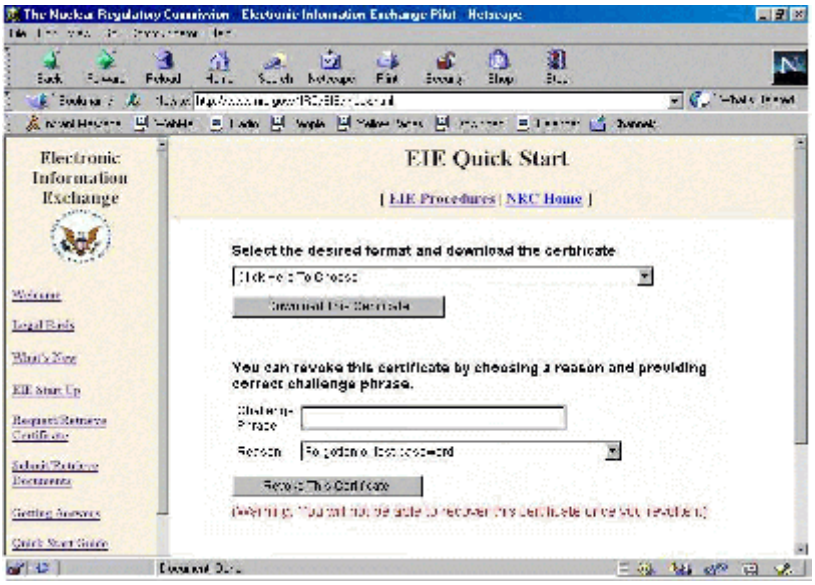

Figure 5-40: Revoke Certificate Page

Step 4: Click on the **Revoke This Certificate** button. When you click Revoke, VeriSign processes the revocation request, revokes the certificate, and updates the VeriSign Certificate Report.

Please note that your revoked Digital ID still shows up in the Digital ID Center's online directory. As the Certification Authority, VeriSign must maintain records on the current status of all Digital IDs issued in the past five years, and must make this information available to the public. This protects you, and any party trusting your digital certificate, against misuse of a compromised or expired Digital ID. Your Digital ID should now appear in the directory as "status: revoked," allowing anyone who might have used your Digital ID to see that your identity can no longer be verified.

5.7 How to Delete Your Digital ID

If your Digital ID is replaced due to expiration or revocation, you may wish to delete the old one. To remove your Digital ID and key files from your machine, follow the steps outlined in Section 5.4, "How to Transfer Your Digital ID to Another Computer."

5.8 Frequently Asked Questions

Netscape Navigator hung when I submitted my request and when I tried to install my Digital ID it didn't work:

When you click the Submit button in the final enrollment page, Navigator sends your Digital ID request and prompts you to specify whether or not you want to enter a password. If you click the Cancel button in this dialog box, Navigator assumes that you want to cancel the entire process and deletes your private key. However, your request has already been sent and a Digital ID generated in response. Because the private key associated with this Digital ID no longer exists, it cannot be installed into Navigator. As a result, canceling out of the password screen causes a long delay and sometimes causes Navigator to hang. Netscape is aware of this problem and it will be addressed in upcoming versions of Navigator. Because the private key is deleted when you cancel out of the password dialog box, attempting to install your Digital ID using will also fail.

To get a Digital ID you will need to complete a new Digital ID enrollment request. Because duplicate Digital IDs are not issued, when you complete the enrollment form for your new Digital ID, you will need to alter the way you enter your name in some way, such as by adding a middle initial or writing your name in all capital letters.

I have enrolled for a Digital ID but, when I look in my security options, it does not show up:

If you did not enter a nickname when saving your Digital ID, then the Digital ID may not appear in your security menu despite being saved in Navigator. Simply click the View button to display the entire Digital ID.

I got the E-mail with my PIN, but I accidentally deleted it before copying my PIN:

The E-mail response to a Digital ID enrollment is automatic. Unfortunately, VeriSign cannot regenerate the PIN information. You will have to enroll for a new Digital ID. Since a Digital ID has already been generated in your name, and since VeriSign cannot generate two identical Digital IDs, you will have to alter your name in some way (e.g. add a middle initial or give your name in all capital letters) in order to get a new PIN sent to your e-mail address.

My PIN does not appear to work:

If possible, use the **Copy** and **Paste** commands from the Edit menu to copy your PIN from the e-mail you received and paste it into the field on the page you use to get your Digital ID. If copying and pasting does not work with your software, and you must type the PIN, make sure:

- the PIN includes 16 or 32 characters,
- the characters include only the numerals 0 (zero) through 9 and the letters A through F, and
- there are no spaces before, after, or within the PIN.

When I try to download my Digital ID, I get the message "private key not found:"

When you retrieve your Digital ID, VeriSign automatically checks to make sure that the private key created in your hard drive during enrollment matches the public key in your Digital ID. In order for these to match, you must be using the same web browser, in the same directory, on the same computer as you were when you requested the Digital ID.

Can somebody else revoke my Digital ID without my knowledge or permission?

No. When you enrolled for your Digital ID you chose a "challenge phrase," which only you should know. To change the status of your Digital ID in any way you have to present this phrase.

I have a new E-mail address. Can I update my Digital ID?

Once a Digital ID has been issued it cannot be changed. Your Digital ID specifically verifies that your public key is bound to your stated e-mail address, so when you change addresses you need to revoke the old Digital ID and request a new Digital ID.

I moved or changed my name. Can I update the information on my Digital ID?

Once a Digital ID has been issued it cannot be changed. If you would like your Digital ID to reflect your new information, you will need to obtain a new one.

Will unplugging my computer disrupt my Digital ID?

No. Your key pair and your Digital ID are stored on your hard drive and are not disrupted by removing the power source to your computer.

Can I use my Digital ID with more than one browser or E-mail application (e.g., with Netscape Navigator and Microsoft Internet Explorer)?

Yes. You may use your Digital ID with more than one browser. To export your Digital ID and import it to another browser, follow the steps outlined in Section 5.4, "How to Transfer Your Digital ID to Another Computer."

Note: There is a bug in some versions of Internet Explorer 4.0 you may be prompted to enter this password multiple times (possibly as many as 20) before it takes. Microsoft is aware of this and is working towards a solution

Import Into Netscape Navigator: **Note:** Only the later versions of Navigator 4.0 and up support importing Digital IDs

I am upgrading Netscape Communicator or to Microsoft Internet Explorer. How do I save my Digital ID?

If you follow the instructions for upgrading your browser provided by Netscape or Microsoft, your Digital ID will be automatically preserved. Do NOT delete your old version of the software before installing the upgrade.

I deleted my old Microsoft Internet Explorer or Netscape Navigator and installed the latest version. How do I reinstall my Digital ID?

If you removed your copy of Microsoft Internet Explorer or Netscape Navigator by deleting the application and its directory, you also deleted the file that contained the private key associated with your Digital ID. Without that private key, you cannot reinstall your Digital ID.

Upgrading with installers preserves your personal information, including your Digital ID and private key. In the future, you should use the installer when upgrading.

Statement of Liability

The provision of an electronic information exchange system by the NRC for the purposes of submitting and transmitting documentary material is based on the terms and conditions outlined below. Those who use the NRC's EIE system do so of their own accord. The exchange of information shall be conducted in good faith among the parties participating. The NRC shall have no responsibility to warrant the authenticity of the information exchanged nor to validate the identity of those involved in the exchange. The NRC shall not be liable in any actions arising from transactions among parties participating in the EIE process in accordance with the authorities and statements of guidance listed below.

- Relevant Federal Regulations

  The use of the NRC EIE Public Certification Services are subject to various U.S. Federal and State criminal laws, which may include but are not limited to: 18 U.S.C. § 1030 (Computer Fraud and Abuse Act of 1986), 18 U.S.C. § 1343 (Federal Wire Fraud Act), 18 U.S.C. § 2701 (Unlawful Access to Stored Communications - The Electronic Communications Privacy Act of 1986), and 18 U.S.C. § 1029 (Fraud and Related Activity in Connection with Computers).

- Exclusion of Certain Elements of Damages

  In no event shall any issuing authority or NRC be liable for any indirect, special, incidental, or consequential damages, or for any loss of profits, loss of data, or other indirect, consequential, or punitive damages arising from or in connection with the use, delivery, license, performance, or nonperformance of certificates, digital signatures, or any other transactions or services offered or contemplated by the NRC, even if such issuing authorities or NRC, or both, have been advised of the possibility of such damages.

- Subscriber Liability to Relying Parties

  Without limiting other subscriber obligations, subscribers are liable for any misrepresentations they make in certificates to third parties who, having verified one or more digital signatures with the certificate, reasonably rely on the representations contained therein.

Glossary of Terms

Access Control List (ACL)	A specific list of individuals or groups that are allowed access to specific areas of the NRC EIE external server.
Certificate Authority (CA)	The trusted authority that creates, assigns, tracks, maintains, and publishes certificates.
Certificate Database	The file which contains your Digital ID certificate within the Netscape Navigator or Communicator browser.
Challenge Phrase	A set of numbers and/or letters that are chosen by a certificate applicant, communicated to the issuing authority with a certificate application, and used by the issuing authority to authenticate the subscriber for various purposes.
Digital ID Certificates	A special data structure that contains a user's unique identification, the user's public key, and some parameters related to the validity of the certificate such as the date of expiration. Digital certificates, with public keys, are maintained openly in a directory in the possession of a certificate or certifying authority (currently VeriSign, Inc.).
Digital Signatures	A digital signature is a checksum which is the result of the application of a secret key and algorithm to a message. As a result, the digital signature is not constant; that is, it always depends on the bit values of the document that it signs. Upon receipt of the document, the digital signature is re-created and compared to the transmitted digital signature. If the signatures match, the sender is authenticated and the document integrity is assured. A non-match indicates that either the document was altered or that the signature is not that of the expected sender.
Encryption Strength	The strength of the encryption depends on the length of the key used. The length of the key is measured in "bits." Generally, longer keys are stronger than shorter keys. Key size ranges from 512 bits to 1024 bits.
Key Generation	The process of creating a private key during certificate application whose corresponding public key is submitted to the Certificate Authority for validation.
Key Pair	A set of encrypted keys composed of a private key and a corresponding public key. The private key is known only to you and is not communicated to the Certificate Authority.

Local Registration Authority (LRA)	NRC staff who identify candidates to be certificate holders and vouches for the binding between public keys and certificate holder identities.
Local Registration Authority Administrator (LRAA)	NRC staff who receives and reviews certificate requests, approves or disapproves certificate requests, notifies the Certification Authority of approve/disapprove decisions, and performs review of requirements related to the digital signatures.
Portable Document Format (PDF)	A standard to make the interchange of formatted documents between differing computing environments as reliable as possible. It is designed to ensure the integrity of the document being interchanged regardless of the computer, operating system, or application software used to create the original document.
Private Key	A mathematical key (kept secret by the holder) used to create digital signatures and, depending upon the algorithm, to decrypt messages or files encrypted (for confidentiality) with the corresponding public key.
Public Key	A mathematical key that can be made publicly available and which is used to verify signatures created with its corresponding private key. Depending on the algorithm, public keys are used to encrypt messages or files which can then be decrypted with the corresponding private key.
Public Key Infrastructure (PKI)	A system for publishing the public-key values used in public-key cryptography. There are two operations common to all PKIs. *Certification* is the process of binding a public-key value to an individual, organization or other entity, or even to some other piece of information, such as a permission or credential. *Validation* is the process of verifying that a certification is still valid.
Secure Hypertext Transfer Protocol (HTTP-S)	HTTP-S provides secure communication mechanisms between an HTTP client/server pair in order to enable spontaneous commercial transactions for a wide range of applications. It provides a flexible protocol that supports multiple orthogonal operation modes, key management mechanisms, trust models, cryptographic algorithms, and encapsulation formats through option negotiation between parties for each transaction.
Secure Sockets Layer (SSL3)	A protocol designed to enable encrypted, authenticated communications across the Internet. URLs that begin with “https” indicate that an SSL connection will be used. In an

	SSL connection, each side of the connection must have a Security Certificate. SSL3 includes three things; privacy, authentication, and message integrity.
Time Stamp	A notation that indicates (at least) the correct date and time of an action, and identity of the person or device that sent or received the time stamp.
Uniform Resource Locator (URL)	A standardized device for identifying and locating certain records and other resources located on the World Wide Web.

Appendix A. Digital Certificate Request Confirmation

From: <jed@nrc.gov>
To: john_smith@abc.com
Date: Fri, Nov 17, 2000 8:00 AM
Subject: Digital ID request confirmation

Dear John Smith,

Thank you for requesting a Digital ID. Your administrator is processing your request, and will notify you when your Digital ID is ready.

If you have questions about your application, please contact your Administrator by replying to this e-mail message.

Appendix B. Digital Certificate Request Disapproval

From: <jed1@nrc.gov>
To: john_doe@abc.com
Date: Fri, Nov 17, 2000 8:27 AM
Subject: Cannot Process Digital ID Request

Dear JOHN Q PUBLIC

Your Administrator was not able to approve your Digital ID/certificate request based on the information you provided.

You may receive another e-mail detailing the specific reasons why your Administrator could not issue your Digital ID. If you have questions, please contact your Administrator by replying to this e-mail message.

Appendix C. Digital Certificate Approval Notification

From: <jed@nrc.gov>
To: john_smith@abc.com
Date: Fri, Nov 17, 2000 9:22 AM
Subject: Your Digital ID is ready

Dear John Smith,

Your Administrator has approved your Digital ID request. To assure that someone else cannot obtain a Digital ID that contains your personal information, you must retrieve your Digital ID from a secure web site using a unique Personal Identification Number (PIN). You can retrieve your Digital ID by following these simple steps:

Step 1: Visit the Digital ID retrieval web page. If your Administrator has set up a customized location for retrieving your Digital ID, you should visit the URL specified by your Administrator. Otherwise, you can retrieve your ID at

https://onsite.verisign.com/USNuclearRegulatoryCommissionADDOCIO/index.html

Step 2: In the form, enter your Personal Identification Number (PIN):

Your PIN is: XXXXXXXXX

Step 3: Follow the instructions on the page to complete the installation of your Digital ID.

If you have any questions or problems, please contact your Administrator by replying to this e-mail message.


UNITED STATES NUCLEAR REGULATORY COMMISSION